Hochschule Macromedia für angewandte Wissenschaften,
University of Applied Sciences

BACHELORARBEIT

zur Erlangung des akademischen Grades
Bachelor of Arts

Chancen und Risiken von Bitcoin als Tausch- und Zahlungsmittel im Studiengang Medienmanagement Studienrichtung Markenkommunikation und Werbung

Erstprüfer:

Prof. Dr. Philipp Riehm

Vorgelegt von:

Vorname Name:	Marc Behlau
Matr.-Nr.:	H-33989
Studiengang:	Medienmanagement
Fachrichtung:	Markenkommunikation und Werbung

Hamburg, 02.02.2018

Zusammenfassung

Die vorliegende Arbeit zielt auf die Identifikation der inneren und äußeren Einflüsse Bitcoins hinsichtlich der weiterführenden Ableitung von dessen Chancen und Risiken in der Nutzung als Tausch- und Zahlungsmittel ab. Herausgearbeitete Erkenntnisse aus bestehender Literatur zur bearbeiteten Disziplin, sowie leitfadengestützte Experteninterviews bilden dabei das Fundament. Die erhobenen Daten wurden mittels einer qualitativen Inhaltsanalyse deduktiv überprüft und analysiert.

Der Arbeit war es möglich herauszufinden, dass sich eine Nutzung des Bitcoins aufgrund mehrerer Risikofaktoren nur in wenigen Fällen empfiehlt. Zum einen entstehen durch systemimmanente Faktoren hohe Transaktionskosten, sowie -zeiten, die eine Nutzung als Tausch- und Zahlungsmittel im Vergleich zu der überwiegenden Anzahl der herkömmlichen Zahlungsmethoden der Währungen weder technisch, noch ökonomisch effizient gestalten. Zum anderen stellt die hohe Volatilität des Bitcoins ein Risiko für Käufer und Verkäufer am Markt dar. Diese Risiken ergeben sich neben der technischen und betriebswirtschaftlichen auch auf der steuer- und finanzrechtlichen Seite. Auch setzt eine Nutzung des Netzwerks technische Affinität voraus.

Es gilt hierbei anzumerken, dass sich die durchgeführte Analyse angesichts der Aktualität des erforschten Bereichs nur auf den derzeitigen Stand der Technologie, sowie die absehbaren Anpassungen dieser bezieht.

Mit dieser Arbeit trägt der Autor zur Schließung der identifizierten Forschungslücke in diesem Bereich bei. Weiterhin werden Maßnahmen für anknüpfende Forschungsmöglichkeiten aufgezeigt.

Abstract

The following graduation thesis aims at identifying the internal and external influences of Bitcoin with regard to the chances and risks as a medium of exchange and payment. Findings from existing literature on the discipline being dealt with, as well as guided expert interviews, provide the foundation. The collected data was deductively checked and analyzed by performing a qualitative content analysis.

On the basis of the results of this research, it can be concluded that usage of Bitcoin can only be recommended in a few cases due to several risk factors. On the one hand, system-inherent factors result in high transaction costs and times, which make this type of exchange and payment method - compared to the vast majority of conventional payment methods - neither technically nor economically efficient. On the other hand, the high volatility of Bitcoin presents a risk for buyers and sellers on the market. These risks come along with technical and economic as well as financial and tax-related issues. Furthermore, using the network requires technical affinity.

It should be noted that, given the novelty of the research area and the incessant development, the analysis carried out only relates to the current state of technology and the foreseeable changes therein.

With this work, the author contributes to closing the identified research gap in this area. Furthermore, possible ways for related research opportunities are delineated.

Schlüsselbegriffe

Bitcoin

Blockchain

Einflussfaktoren

Tausch- und Zahlungsmittel

Währung

Keywords

Bitcoin

Blockchain

Currency

Influence factors

Means of exchange and payment

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BTC	Bezeichnung für Bitcoin an vielen Handelsplätzen
EStG	Einkommenssteuergesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GE	Geldeinheit
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbH & Co. KG	Gesellschaft mit beschränkter Haftung & Compagnie Kommanditgesellschaft
ICO	Initial Coin Offering
IT	Informationstechnologie
MB	Megabyte
PoW	Proof of Work
PoS	Proof of Stake
USA	United States of America
ZB	Zentralbank
EZB	Europäische Zentralbank

1. Einleitung

Das Aufkommen des Internets leitete eine neue Ära von günstigen, schnellen und effizienten Möglichkeiten der Durchführung von Zahlungen ein. In den 90er Jahren, als sich dieses langsam zu entwickeln begann, forschten dabei viele Wissenschaftler an weiteren Anwendungsbereichen dieser neuen Technologie und den möglichen Auswirkungen dieser auf die Gesellschaft. Eine viel theorisierte stellte dabei der Entwurf von Internetgeld dar. Davidson (1997) sprach dabei, als einer von vielen, über internetbasiertes Geld, welches auf einem Computer gespeichert und über das Internet transferiert, Papiergeld obsolet machen würde: „Unique, anonymous, and verifiable, this money will accomplish the largest transactions. It will also be divisible into the tiniest fraction of value and be tradable at a keystroke […].” (S. 215) (Macintosh, 1998, S. 739–796). Mit dem Abklingen der Neuartigkeit des Internets und dem damit einhergehenden Abebben des Hypes ließen die Forschungen an dem Potenzial eines solchen digitalen Geldes jedoch nach. Trotz des Voranschreitens der Digitalisierung der Gesellschaft, war lange Zeit kein Wachstum in diesem Bereich zu verzeichnen.

Im Jahr 2009 kam jedoch die erste Ausprägung dieser oft vorausgesagten Technologie auf: Die Entwicklung des ersten digitalen, kryptographischen und Peer-to-Peer[1] basierten Tausch-und Zahlungsmittels: Bitcoin. Dieses Medium stellte die erste mögliche Alternative gegenüber staatlichen Währungen und nutzbaren digitalen Zahlungsmitteln dar, deren Ermittlung etwaiger Chancen und Risiken in der Nutzung Bitcoins als Zahlungsmittel sich diese Arbeit annimmt. Derzeit lassen sich dabei über 16.8 Millionen Bitcoin im Umlauf[2] identifizieren, die zusammen einen Marktwert von über 268 Milliarden Euro[3] erreichen. Diese hohen Werte können auf das starke Interesse des Marktes an diesem neuen Medium und seiner zugrundeliegenden Technologie, der Blockchain, zurückgeführt werden. Fraglich ist jedoch, ob das als Tausch- und Zahlungsmittel konzipierte Werkzeug auch bei einer hohen Marktkapitalisierung[4] skalieren kann und ob sich in dessen Nutzung Vorteile ergeben, die eine Nutzung als solches ökonomisch rechtfertigen. Die Identifikation eines solchen *sozialen Problems* fordert in der Empirie die Durchführung einer Forschungsarbeit (Mayring, 2002, S. 24). Von diesem Problem ausgehend lässt sich die folgende wissenschaftliche Fragestellung ableiten, welche es im Laufe des Forschungsprozesses fundiert zu beantworten

---

[1] Eine Peer-to-Peer Verbindung ist als eine gleichberechtigte Kommunikation zwischen Computern eines Netzwerks zu verstehen - engl.: peer = Gleichgestellter (Steinmetz, 2004, S. 51-54).
[2] Marktkapitalisierung des Bitcoin: Stand 05.01.2018 (CoinGecko, 2018).
[3] Marktwert aller Bitcoin: Stand 05.01.2018 (Coingecko, 2018)
[4] Unter Marktkapitalisierung wird die gesamte Anzahl der Bitcoins am Markt verstanden (Wildmann, 2007, S. 115 ff).

gilt: *Welche Chancen und Risiken ergeben sich in der Nutzung von Bitcoin als Tausch- und Zahlungsmittel*?

Der Ursprung der Forschungsfrage lässt sich hierbei sich auf den Besuch einiger Internetforen zurückführen, in denen Bitcoin-Diskussionen stetig an Gewichtung zu gewinnen begannen. Die überwiegende Anzahl dieser drehte sich um Preisspekulationen und die Auswirkungen der Blockchain-Technologie Bitcoins auf etliche Bereiche der Wirtschaft. Weitere Diskussionen drehten sich um die Frage, wann und in welchen Bereichen sich Bitcoin als Zahlungsmittel durchsetzt. Auch eine ausgedehnte Recherche führte zu dem gleichen Ergebnis. Ob das Netzwerk jedoch über die technische Architektur verfügt, die eine globale Skalierung von Transaktionen zu geringen Kosten ermöglichen kann, blieb offen.

Der Ursprungsgedanke Bitcoins, Intermediäre obsolet zu machen, und ein daraus resultierendes System mit geringen Kosten, durch den Wegfall von zentralen Steuereinheiten, und einer unangreifbaren Sicherheitsstruktur zu erschaffen, scheint heute nur teilweise erfüllt. Transaktionskosten haben eine Höhe erreicht, die Zahlungen in vielen Fällen unwirtschaftlich gestalten können. Ob Bitcoin dementsprechend das Potenzial besitzt, die Aufgabe des Kerngedankens effizient zu erfüllen, wurde bisher in der bekannten Forschung nicht identifizierbar untersucht, da die öffentliche Aufmerksamkeit den Fokus weitestgehend auf den Preisanstieg des Mediums gelegt zu haben scheint, und die Nutzung als Tausch-und Zahlungsmittel am Markt bisher wenig Akzeptanz gefunden hat. Für die zu beantwortende spezielle Forschungsfrage hält die Wissenschaft aus diesem Grund nur bedingt theoretische Grundlagen und etwaige Forschungsergebnisse für den genannten Verwendungszweck Bitcoins bereit.

Vor dem Hintergrund dieser ermittelten Forschungslücke stellt das Ziel dieser Arbeit dementsprechend den Beitrag von neuen Erkenntnissen in dem zu untersuchenden Bereich dar. Der Autor wendet hierbei ein wissensaneignendes Forschungsdesign an. Um eine korrekte Durchführung der empirischen Untersuchung in Form von Experteninterviews und einer qualitativen Inhaltsanalyse zu gewährleisten, gilt es vorab die theoretischen Grundlagen zu ermitteln. Zur Untersuchung der Forschungsfrage werden daher einführend Bitcoin und die Blockchaintechnologie analysiert und deren Hauptaspekte identifiziert. Zusätzlich bedarf es eines Vergleichs mit den bisher konkurrenzlosen und zentral gesteuerten digitalen Tausch-und Zahlungsmitteln am Markt, den Währungen, um in Zuge dessen die *Chancen und Risiken von Bitcoin als Tausch- und Zahlungsmittel* abzuleiten.

Um Chancen dabei als eine mögliche Förderung und Risiken als eine mögliche Gefährdung wahrzunehmen, bedarf es vorab einer Definition der genannten Begriffe.

„Unter einem Risiko versteht man in der Betriebswirtschaft, dass in der Folge einer zu treffenden Entscheidung verschiedene relevante Umweltsituationen mit jeweils entweder objektiv zu ermittelnden oder subjektiv zu schätzenden Wahrscheinlichkeiten eintreten können.“ (Bieder, 2011, S. 13ff). In dem, in dieser Arbeit zu betrachtenden, System geht mit dem Risiko eine materielle oder monetäre Verlustgefahr einher, derer es vorzubeugen gilt. Unberücksichtigt soll hierbei die von der Situation des Risikos abzugrenzende Unsicherheit bleiben. Unter einer Unsicherheit im betriebswirtschaftlichen Kontext wird eine Situation verstanden, in der durch den Mangel an subjektiven und/oder objektiven Aussagen über Eintrittswahrscheinlichkeiten von möglichen Zuständen keine ausreichend gedeckten Vorhersagen über künftige Begebenheiten getroffen werden können (Busse von Colbe, 1991, S.32; Laux, 2007, S.23).
Als Chance lässt sich anschließend der inverse Zustand von einem Risiko, dem Eintritt eines erwünschten Ereignisses definieren (Stocker, 2006, S.10).

2. Theoretische Grundlagen der Analyse

Im Rahmen dieses Kapitels werden die notwendigen theoretischen Grundlagen erarbeitet, welche in Bezug auf die Analyse der Chancen und Risiken von Bitcoin als Tausch- und Zahlungsmittel für den Hauptteil dieser Arbeit relevant sind. In diesem Zuge werden im weiteren Verlauf die beiden Themen Bitcoin und Fiat-Währungen, sowie deren Zahlungsmethoden behandelt.

2.1. Überblick

Um die Chancen und Risiken von Bitcoin als Tausch-und Zahlungsmittel zu identifizieren, ist es vorab notwendig, ein Verständnis der Funktionsweise der Technologie Bitcoins zu schaffen und dieses in Verbindung mit den herkömmlichen Tausch-und Zahlungsmitteln am Markt, den staatlichen Währungen, zu bringen, um anschließend im Zuge einer Anreicherung des Wissens durch leitfadengestützte Experteninterviews, sowie einer qualitativen Inhaltsanalyse die Leitfrage fundiert beantworten zu können.

In dem folgenden Abschnitt erfolgt zunächst eine Begriffserklärung für *Bitcoin* und dessen *Blockchain*, sowie eine Begriffsabgrenzung von dem Begriff *Distributed Ledger*. Daraufhin erfolgt eine Darstellung der Funktionsweise und die daraus resultierenden wesentlichen Merkmale der Blockchain-Technologie. Den Abschluss des Kapitels bildet eine Zusammenfassung der, im Rahmen dieses Kapitels gewonnenen, theoreti-

schen Erkenntnisse im Hinblick auf die Ableitung der (Hypo-) These(n), welche die Grundlage für die anschließende Datenerhebung, sowie deren Auswertung mittels einer qualitativen Analyse darstellen.

2.2. Bitcoin

Im Jahre 2008 gelang es einem Individuum oder einer Gruppe, bekannt unter dem Pseudonym Satoshi Nakamoto, ein bis zu dem Zeitpunkt ungelöstes Problem der Computerwissenschaft, das *Byzantine Generals Problem*[5], zu entschlüsseln. Das Whitepaper[6] *Bitcoin: A Peer-to-Peer Electronic Cash System*, veröffentlicht in der *Cryptography Mailing List*[7] beschreibt die Funktionsweise von Bitcoin. Durch die Lösung dieses Informatikproblems konnte erstmalig Knappheit in einem digitalen Umfeld erlangt werden (Nakamoto, 2008. S.1 ff). Zusammengefasst bedeutet dies, dass im Falle einer Transaktion der Empfänger sichergehen kann, dass der Sender das Übermittelte nicht mehr besitzt. Hierunter wird auch die Schaffung digitaler Knappheit verstanden (Platzer, 2016). Das galt bisher als unmöglich, da jeder im Internet Daten in beliebiger Anzahl vervielfältigen kann, ohne Nachweis ob und/oder wie oft dies erfolgt war. Mit dem Bitcoin-Protokoll kann diese Art der Knappheit jedoch erreicht werden. Am 9. Januar 2009 veröffentlichte Nakamoto Version 0.1 der Bitcoin Software und gründete die Webseite *bitcoin.org*. Nakamoto arbeitete an der Software bis Mitte 2010 weiter und übergab anschließend Gavin Andresen[8] den kompletten Source Code bevor er/sie sich zurückzog(en), welcher zusammen mit weiteren Mitgliedern der Bitcoin Community den Code bis heute weiterentwickelt. Bitcoin vereint drei technologische Ebenen. Erstens die Blockchaintechnologie, das dezentrale und transparente Verzeichnis, zweitens das Bitcoin Protokoll, die Software, die festlegt, wie Assets[9] auf der Blockchain transferiert werden und drittens das Asset Bitcoin selbst (Swan, 2015, S. 12ff)

Als weltweit erstes Krypto-Asset[10] mit der breitesten Akzeptanz wird Bitcoin, im Gegensatz zu Währungen wie dem Dollar oder dem Euro nicht von einer Zentralbank ausgegeben und verwaltet, sondern von einem dezentralisierten Netzwerk, an welchem jeder teilhaben kann, der die Bitcoin-Software auf einem Computer mit Internetverbindung

[5] (Kapitel 2.2.2)
[6] Bei einem Whitepaper handelt es sich um ein Dokument, welches die Ziele und Funktionsweise eines angestrebten Projektes darstellt.
[7] International anerkanntes Medium des Austausches über themenrelevante Forschungsentwicklungen im Bereich der Kryptographie (Nakomoto Institute, 2008).
[8] Einer der ersten Softwareentwickler Bitcoins und bis Februar 2016 Leiter des Entwicklungsteams (Simonite, 2014; Todd, 2016).
[9] Als Asset wird jegliche ökonomische Ressource klassifiziert, die einen Wert erhalten kann (O´Sullivan, 2003, S. 272; Bakshi, 2013, S. 139–163).
[10] Bitcoin ist als hybrides, kryptographisches Asset zu definieren (Kapitel 2.3.2).

ausführt. Das mathematische Protokoll ist unveränderlich und garantiert nicht verletzbare Regeln im System, unter anderem die maximal erzeugbare Anzahl von 21 Millionen BTC. Diese Endlichkeit verleiht dem Bitcoin einen deflationären Charakter. Bei der Preisgestaltung des Bitcoin handelt es sich um flexible Wechselkurse am Markt, ähnlich wie bei dem Handel mit Aktien. Angebot und Nachfrage bestimmen den Preis. Im Gegensatz zu souveränen staatlichen Währungen existieren Bitcoins dabei rein virtuell und können bis auf die achte Nachkommastelle genau angegeben werden. Die Maßeinheit für diese Nachkommastellen wird als *Satoshi* [11] bezeichnet. 1 Satoshi entspricht dabei 0.00000001 BTC.

2.2.1. Begriffsabgrenzung

Die Begriffe *Blockchain-Technologie* und *Distributed Ledger Technology* (DLT) werden in der öffentlichen Diskussion oft als Synonym verwendet. Distributed Ledger Technology ist jedoch nur als Oberbegriff zu verstehen und bezieht sich auf alle Technologien, die eine auf mehrere Medien verteilte, Datenbank als Basis nutzen. Die Blockchaintechnologie ist als eine Ausprägung dieser zu begreifen.

2.2.2. Das Dilemma der Byzantinischen Generäle und Double-Spending

Abgesehen von den diversen Anwendungsmöglichkeiten, die die Blockchaintechnologie in den verschiedensten Bereichen der Wirtschaft bietet, ist vor allem die Lösung des erwähnten *Double-Spend-Problems*, oder auch des *Byzantine Generals Problems* ein großer kryptographischer[12] Fortschritt. Die Architektur der Blockchaintechnologie baut auf dem Fundament von 20 Jahren Forschung im Bereich der kryptographischen Währungen und über 40 Jahren Forschung im Bereich der Kryptographie selbst auf. Mit Bitcoin führte Nakamoto dieses Wissen zusammen und ergänzte es, sodass das Problem der doppelten oder mehrfachen Vervielfältigung von Daten über das Internet gelöst werden konnte (Swan, 2015, S. 12). Vor der Blockchaintechnologie konnte ohne das Wirken eines zentralen Intermediären über das Internet nicht sichergestellt werden, dass eine solche Vervielfältigung stattfindet. Es bedurfte einer dritten Partei, die das Verzeichnis der Transaktionen zentral speichert und sichergeht, dass das Geld nur einmal ausgegeben werden konnte. Dieses Problem stellt das Double-Spending dar und ist dem Dilemma der Byzantischen Generäle ähnlich. Dieses beschreibt die Herausforderung verschiedener Parteien (Generäle), die sich, auf dem Schlachtfeld befindend, gegenseitig nicht vertrauen, um zu siegen jedoch vertrauensunabhängig

[11] Die Namensgebung der Maßeinheit lässt sich auf den/die Urheber Bitcoins Satoshi Nakamoto zurückführen (Nakamoto, 2009).
[12] Unter Kryptographie versteht man die Kunst der Kommunikation über verschlüsselte Nachrichten (Dannen, 2017, S.2 ff)

miteinander kommunizieren müssen (ebd.). Durch die in den folgenden Kapiteln erläuterte Funktionsweise der Technologie ist dies nun durch das Aufkommen Bitcoins möglich. Die Kombination von Peer-to-Peer Datenübertragung und die Nutzung von Kryptographie machen nur ein Vertrauen in das öffentlich einsehbare Protokoll der Blockchain notwendig, in die andere Partei jedoch nicht (Steinmetz, 2004, S. 51-54).

2.2.3. Blockchaintechnologie

Der Autor bezieht sich in der folgenden Erklärung der Funktionsweise Bitcoins zum größten Teil auf die Werke der Autoren Beehmaiah (2017), Kippenhahn (2012), Swan (2012) und Raval (2016) (S. 7 ff; S. 19 ff; S. 10 ff, S. 6 ff). Weitere Vergleiche und Zitate werden entsprechend gekennzeichnet.

Die Blockchain Bitcoins ist als dezentrale Datenbank zu verstehen, welche alle jemals ausgeführten Transaktionsvorgänge unveränderbar abgespeichert hat. Die Technologie erlaubt es, Handelspartnern, unter welchen kein Vertrauen Bestand haben muss, Transaktionen sicher über ein Peer-to-Peer-Netzwerk abzuwickeln. Bei den Teilnehmern des Systems wird zwischen Minern und Nodes[13] unterschieden. Miner (Kapitel 2.2.4.3.1) stellen die Rechenleistung für die Sammlung und Gruppierung der ausstehenden Transaktionen in Datenblöcke bereit und versuchen ihren Block zu verifizieren. Der Miner, der seinen Block als erstes verifiziert, erhält für die Investition seiner Rechenleitung Bitcoin in Form eines *Block-Rewards*. Dies wird auch als *Schöpfen* oder *Minen* bezeichnet und geschieht alle 10 Minuten (ebd.). Die Höhe dieser Belohnung wird alle vier Jahre halbiert und liegt derzeit bei 12.5 BTC. Anschließend kommuniziert der Miner seinen Block an die Nodes, welche dessen Richtigkeit verifizieren und diesen an den vorherigen Block anketten. Dies geschieht in chronologischer, linearer Ordnung. Diese Kette der Blöcke stellt die Aufzeichnungen aller Transaktionen bis hin zum ersten Genesis-Block[14], dar und bildet die Blockchain, welche von den Nodes identisch gespeichert wird. Diese Kombination von Minern und Nodes bewerkstelligt einen Wegfall von Intermediären. Die Eigenschaft eines öffentlich einsehbaren Verzeichnisses schafft Transparenz in dem Netzwerk, durch welche alle Transaktionen, die mit der jeweiligen Bitcoin-Adresse verknüpft sind, öffentlich über

[13] Bei einer Node handelt es sich um einen an das Bitcoin-Netzwerk angeschlossenen Computer, welcher durch das heruntergeladene Bitcoincomputerprogramm die Funktion der Validierung und Weiterleitung der Transaktionen übernimmt. Jede Node lädt automatisch eine komplette Kopie der Blockchain herunter und ergänzt diese fortlaufend um den folgenden, validierten Block (Raval, 2016, S. 29; Kapitel 2.2.3.5).

[14] Der Block mit der ersten, jemals durchgeführten Transaktion.

einen Blockexplorer[15] eingesehen werden können. Mittels Einsatz von Kryptographie wird zusätzlich eine hohe Netzwerksicherheit hergestellt, erreicht durch die Nutzung von fälschungssicheren Schlüsselpaaren, den Public- und Private-Keys[16], welche den Nachweis für den eindeutigen Besitz einer Position auf der Blockchain ermöglichen, sowie Hash-Funktionen, welche einen Einsatz dieser Schlüssel im System zusätzlich absichern.

2.2.4. Funktionsweise der Blockchain

2.2.4.1. Kryptographie

Unter Kryptographie versteht man die Verschlüsselung von Informationen, welche in diesem Fall die Transaktionen und die Zugänge der Blockchain darstellen (Diffie; Hellmann, 1976, S. 644-654). Aufgrund der Transparenz des Netzwerks, in welchem alle Transaktionen und Adressen eingesehen werden können, ist eine Verschlüsselung dieser unumgänglich. Dem Bitcoinnetzwerk liegt dabei die intensive Nutzung von Kryptographie zugrunde, welche die Sicherheit der Nutzung des Systems gewährleistet. Bei staatlichen Währungen fällt diese Aufgabe den Zentral- und Geschäftsbanken zu, die als zentrale Entität die Sicherheit der Transaktionsvorgänge und Konten gewährleisten. Dazu gehört vor allem das beschriebene Problem des Double-Spendings. Im Regelwerk Bitcoins ist dabei klar definiert, welche Transaktionen gültig sind und wer dabei als der korrekte Empfänger gilt. Diese Regeln werden durch das Protokoll durchgesetzt und bedürfen keinem zentralen Intermediär. Die wichtigste Komponente stellt dabei eben diese Kryptographie dar. Die transferierten Informationen werden verschlüsselt verschickt und können nur von der jeweiligen Partei eingesehen werden. Das Verständnis der Funktionsweise dieser Prozesse ist essentiell, um die *Chancen und Risiken von Bitcoin als Tausch-und Zahlungsmittel* zu erschließen. Im Folgenden werden daher die zentralen kryptographischen Elemente der Technologie dargelegt: Digitale Signaturen und Hash-Funktionen. Digitale Signaturen ermöglichen eine Fälschungssicherheit von Transaktionen und gewährleisten eine Nachweisbarkeit der Identität von Sender und Empfänger. Hash-Funktionen tragen dabei maßgeblich zu einer sicheren Nutzung dieser Signaturen bei.

2.2.4.2. Digitale Signaturen

Für die Verschlüsselung von Nachrichten waren lange Zeit nur symmetrische Verschlüsselungssysteme im Einsatz. Diese gehen bis auf die Zeiten Gaius Julius Cäsars

---

[15] Bei einem Blockexplorer handelt es sich um eine Schnittstelle, wie u.a. einer Node oder einer Webseite (Bsp.: https://blockchain.info/) über welche auf die Blockchain zugegriffen werden kann.

[16] (Kapitel 2.2.4.2)

zurück, der eine Form der symmetrischen Verschlüsselung als Werkzeug für geheime militärische Korrespondenz nutzte (Sing, 1999, S.39). Bei symmetrischen Verschlüsselungen wird zur Ver- und Entschlüsselung der gleiche mathematische Schlüssel verwendet. Der Besitz des Schlüssels ermöglicht demnach einen Zugriff in beide Richtungen. Dazu muss die Verschlüsselungsinformation zwischen zwei Kommunikationspartnern jedoch auf möglichst sicherem Weg überbracht werden. Hinzu kommt, dass bei steigender Anzahl der Kommunikationspartner die benötigte Anzahl der Schlüssel exponentiell zunimmt, sofern nicht jeder Teilnehmer alle Inhalte entschlüsseln können soll (Diffie & Hellmann, 1976, S. 646). Dies bringt also zusätzliche Schwierigkeiten mit sich. Ein Durchbruch gelang in der Informatik Anfang der 70er Jahre mit der Entwicklung asymmetrischer Verschlüsselungssysteme.

Unter asymmetrischer Kryptographie versteht man dabei das Senden sicherer Nachrichten in einem Netzwerk, in dem sowohl der Sender, als auch der Empfänger dem genutzten Kanal misstrauen. Im Falle der Bitcoin-Blockchain stellen diese Nachrichten Transaktionen dar, die signiert und an das Netzwerk kommuniziert werden, um den aktuellen Zustand der betroffenen Accounts zu verändern (Dannen, 2017, S. 26). Beide Beteiligten besitzen dabei zwei verschiedene, mathematisch zusammenhängende Schlüssel, auch bekannt als "Keys". Hierbei gibt es jeweils einen Public und einen Private Key. Entwickelt für die Kommunikation in Kriegszeiten stellt die Public Key Kryptographie ein enorm sicheres Mittel der Informationsübermittlung dar. Im Gegensatz zur symmetrischen Verschlüsslung, bei der sowohl der Sender, als auch der Empfänger den gleichen Key nutzen, um eine Nachricht zu ver- und entschlüsseln, beruht das System der Public Keys, auch bezeichnet als asymmetrische Kryptographie, auf dem Misstrauen des genutzten Kanals. Dieser Punkt gilt als besonders wichtig für die Blockchain, da in dieser jeder beliebige Computer, der das jeweilige Blockchain-Protokoll ausführt, dem Netzwerk ohne Sicherheitsprüfung beitreten kann (Dannen, 2017, S.56). Die daraus resultierende Wichtigkeit des Einsatzes von Verschlüsselung wird durch das Verwenden von Public und Private Keys berücksichtigt.

Hierbei gibt das System zwei Keys gleichzeitig heraus. Der erste Schlüssel, der Public Key, ist öffentlich. Dieser kann beliebig im Internet geteilt werden und fungiert als Adresse. Der zweite Schlüssel, der Private Key, fungiert als persönliche Unterschrift (digitale Signatur) und muss geheim gehalten werden, da dieser als Beweis für den Besitz des Eintrags im Blockchain-Verzeichnis, also des Kontos innerhalb der Blockchain agiert. Dies kann analog mit einer Unterschrift des Senders auf einem Brief vergleichen werden, da diese den Sender eindeutig identifiziert und von allen gelesen

werden kann, jedoch schwer zu fälschen ist, wobei Private-Keys keine fälschbaren Eigenschaften aufweisen.
Die Schlüssel können als zusammenhängende Paare gesehen werden. Der Private Key kann Nachrichten, die durch den passenden Public Key verschlüsselt wurden, entschlüsseln und umgekehrt. Dies ist möglich, da die Schlüsselpaare füreinander generiert werden und so konzipiert sind, dass mit einem dieser Keys verschlüsselte Informationen immer durch den anderen entschlüsselt werden können.

Der kryptographische Prozess wird im Folgenden anhand eines Beispiels dargelegt:
Wie in Abbildung 1 zu erkennen haben wir einen Sender "Alice" und einen Empfänger "Bob". Alice möchte ihre Nachricht verschlüsseln und an Bob versenden. Dabei möchte sie sicherstellen, dass nur Bob diese lesen kann und gleichzeitig weiß, dass die Nachricht unzweifelhaft von ihr stammt. Alice verschlüsselt diese daher zuerst mit ihrem Private Key und anschließend erneut mit Bobs Public Key.

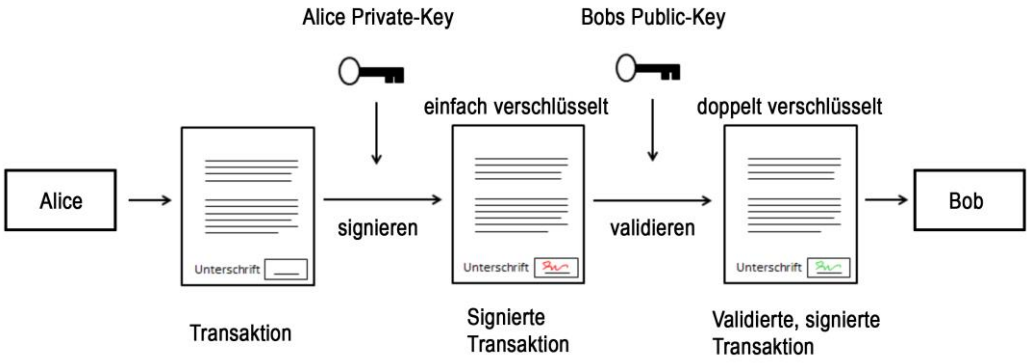

Abbildung 1: **Digitale Signaturen - Verschlüsselung.** Quelle: Eigene Abbildung, 2018.

Die Nachricht enthält nun also eine Verschlüsselung durch ihren Private Key, welchen nur Alice besitzen kann. Dieser Vorgang wird auch als digitale Signatur bezeichnet. Das beweist Alice Identität als Sender, welche Bob über Alice Gegenstück, ihren Public Key, verifizieren kann. Zusätzlich enthält die Nachricht eine Verschlüsselung durch Bobs Public Key, welche nur Bob mit seinem Private Key entschlüsseln kann. Daher entschlüsselt Bob zuerst die Nachricht mit seinem Private Key und hinterher erneut mit Alice Public Key (siehe Abbildung 2).

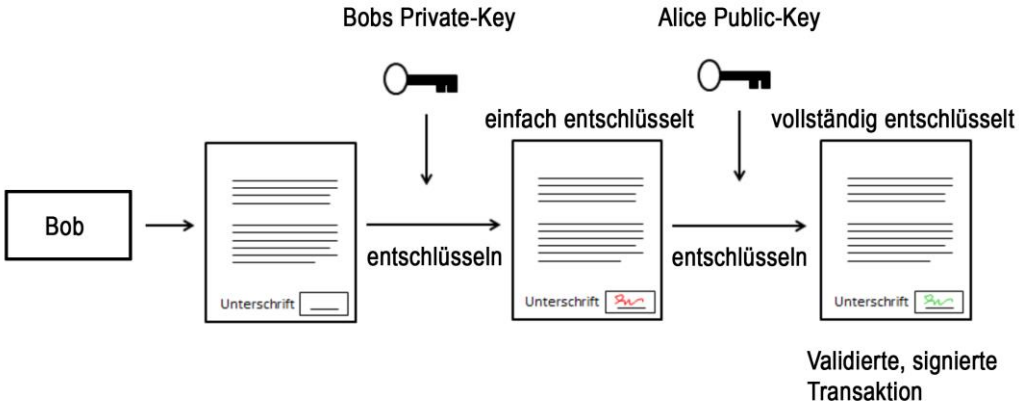

Abbildung 2: **Digitale Signaturen – Entschlüsselung.** Quelle: Eigene Abbildung, 2018.

Diese beiden Sicherheitsebenen ermöglichen eine kryptographisch vollkommen gesicherte Kommunikation.

2.2.4.3. Kryptographisches Hashing

Um eine größtmögliche Sicherheit zu erreichen, nutzt Alice zusätzlich noch eine Hashfunktion um die gesendete Nachricht zusätzlich zu sichern. Hash-Funktionen sind mathematische Funktionen, bei denen folgende Eigenschaften identifiziert werden können:

- Der Eingabewert ist eine beliebige Eingabemenge mit beliebiger Länge.
- Der Hashwert, also der Ausgabewert, weist eine vordefinierte Größe auf und beträgt im Fall des Bitcoin-Algorithmus immer 256-bit.
- Der gleiche Eingabewert führt nach Anwendung des Algorithmus immer zu dem gleichen Hash-Wert. Demnach ist eine Hash-Funktion als deterministisch einzustufen.
- Der benötigte Rechenaufwand muss geringgehalten werden.

Bei einem Hash-Wert handelt es sich demnach um einen Wert fester Länge, welcher als Hexadezimale-Zeichenkette[17] dargestellt wird und aus allen erdenklichen Eingabewerten erstellt werden kann. Der Hash-Wert wird durch einen Algorithmus berechnet, der eine beliebige Eingabemenge mit beliebiger Länge auf eine Zielmenge mit

[17] Das Hexadezimale Zahlensystem wird überwiegend in der IT verwendet und besteht aus den 16 Ziffern 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E und F.

festgelegter Länge abbildet (siehe Abbildung 3).

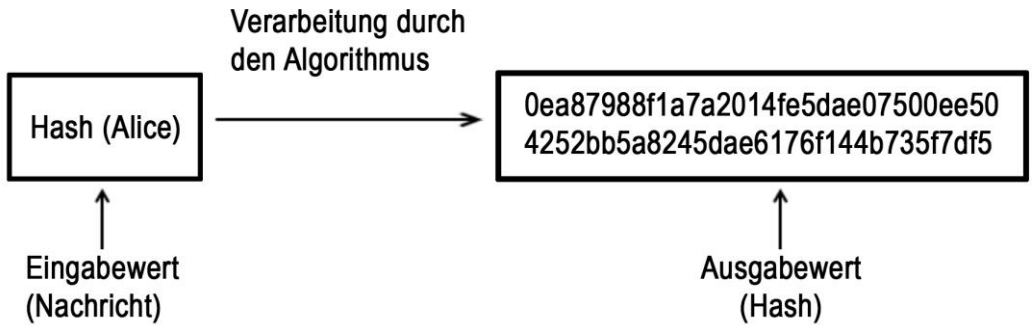

Abbildung 3: **Hash-Funktion - Eingabewert - Hash (Alice).** Quelle: Eigene Abbildung, 2018.

Eine kleine Änderung ergibt dabei, wie in Abbildung 4 zu erkennen, einen vollkommen anderen Hash-Wert.

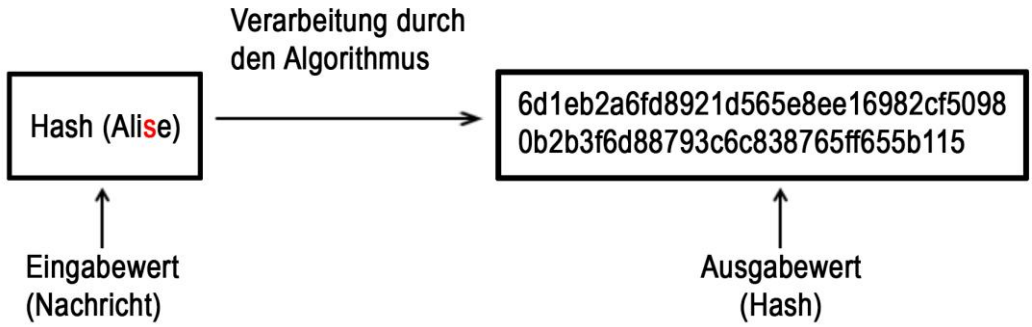

Abbildung 4: **Hash-Funktion - Eingabewert - Hash (Alise).** Quelle: Eigene Abbildung, 2018.

Dementsprechend ist die zentrale Eigenschaft eines Hashwertes, dass durch ihn keine Rückschlüsse auf den ursprünglichen Eingabewert möglich sind. Aus einer festgelegten Zeichenfolge entsteht zwar immer der gleiche Hash-Wert, umgekehrt kann aus diesem die Zeichenfolge jedoch nicht wieder errechnet werden. Diese Eigenschaft macht Hash-Werte für die Speicherung von Passwörtern oder anderen schützenswerten Daten oder Transaktionen sehr wertvoll. Neben der Blockchain findet diese Technik auch in diversen anderen Bereichen ihre Anwendung, wie zum Beispiel bei Betreibern von Domains. Diese speichern nur die Hashwerte der von den Nutzern erstellten Passwörter. Meldet sich ein Nutzer mit seinem Passwort auf der Webseite an, so errechnet das System den Hash-Wert und gleicht diesen mit dem im System gespeicherten Wert ab. Durch diese Art der Datenspeicherung wird einem möglichen Missbrauch von persönlichen Daten nach einer illegalen Aneignung von Daten, beispielsweise durch einen Hackerangriff, vorgebeugt (Sing, 1999, S. 42). Um eine

kryptographische Nutzbarkeit einer Hash-Funktion zu gewährleisten, muss diese zusätzlich drei weitere Eigenschaften aufweisen:

1. Kollisionsresistenz
2. Keine Möglichkeit des Ziehens von Rückschlüssen auf den Eingabewert
3. Effiziente Einbettung in mathematischen Aufgaben

2.2.4.3.1. Kollisionsresistenz

Kollisionsresistenz ist eine unabdingbare Eigenschaft, um eine Hash-Funktion kryptographisch zu verwenden. Eine Kollision entsteht, wenn zwei unterschiedliche Eingabewerte den gleichen Hash-Wert zur Folge haben. Weist eine Funktion keine Kollision auf, so kann diese als kollisionsresistent eingestuft werden. Abbildung 5 stellt eine Kollision zweier Hash-Werte dar. Die verschiedenen Eingabewerte Bob (x) und Alice (y) bekommen durch den Algorithmus die gleichen Hash-Werte.

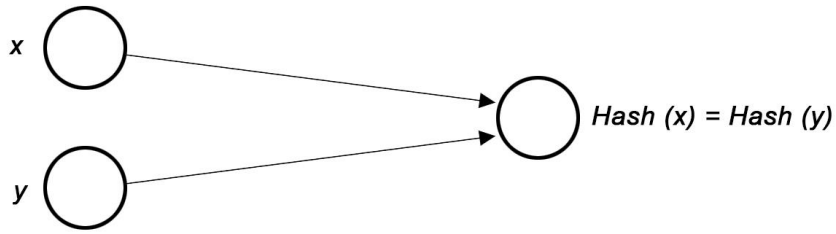

Abbildung 5: **Kollision zweier Hashes.** Quelle: Eigene Abbildung, 2018.

Eine Kollisionsresistenz bedeutet jedoch nicht, dass Kollisionen niemals auftreten können. Hierbei spricht man mathematisch von Kollisionsfreiheit. Aufgrund der Möglichkeit, Eingabewerte mit beliebiger Größe zu nutzen und der Tatsache, dass der Ausgabewert eine vordefinierte hexadezimale Länge aufweist lässt sich schlussfolgern, dass der Bereich der Eingabewerte unendlich, der Bereich der möglichen Ausgabewerte jedoch endlich ist. Demnach muss es zu irgendeinem Zeitpunkt zu einer Kollision kommen. Diese Wahrscheinlichkeit des Eintretens einer solchen Kollision beträgt bei einem 256-bit Hash: 2^{128}. Demnach bräuchte ein Computer mit einer durchschnittlichen Rechenleistung von ungefähr 10.000 Hashes pro Sekunde 2^{27} Jahre, um einen Durchlauf zu beenden, in dem er eine Kollision aufweisen kann (Raval, 2016, S. 64 ff). Zusammengefasst bedeutet dies, dass die Wahrscheinlichkeit einer Kollision theoretisch besteht, jedoch so enorm gering ist, dass dieses Phänomen durchschnittlich alle 10 Milliarden Jahre auftritt (ebd.). Wurde bei einer Hash-Funktion trotz großer

Bemühungen keine Kollision nachgewiesen, gilt diese somit als Kollisionsresistent. Kollisionsfreiheit, die theoretische Möglichkeit einer Kollision, besteht jedoch weiterhin.

Eine Kollisionsresistenz ist für die kryptographische Nutzung insofern von Nöten, dass sie sowohl Fälschungssicherheit garantiert und Betrug vorbeugt, als auch Speicherplatz erheblich reduziert, da das Netzwerk eindeutige Rückschlüsse auf die Korrektheit der Daten ziehen kann, ohne diese zwangläufig kennen zu müssen.

2.2.4.3.2. Einwegfunktionen

Damit keine Rückschlüsse auf den Eingabewert einer Hash-Funktion gezogen werden können, müssen diese die Eigenschaft einer Einwegfunktion aufweisen. Als Grundlage asymmetrischer Kryptographie lassen Einwegfunktionen durch das Hinzufügen einer *Nonce*, einem zufälligen Wert, von dem Hash-Wert nicht auf dessen Eingabewert schließen. Dieser Prozess ist als *Commitment-Verfahren* bekannt und setzt sich aus zwei verschiedenen Algorithmen zusammen:

1. *Commit (Nonce und Eingabewert)*: Durch die Commit-Funktion wird der Eingabewert mit einem zufälligen Wert (Nonce) verkettet. Ergebnis dieser Funktion ist das *Commitment*.
2. *Verify (Nonce, Eingabewert und Commitment)*: Durch die Verify-Funktion werden die Nonce, der Eingabewert und das Commitment verkettet.

Der Eingabewert des Commitments kann bekannt gemacht werden, indem die Nonce bereitgestellt wird. Mit diesem Wert kann der Inhalt der Funktion bestätigt und verifiziert werden. Bezogen auf die vorgestellte kryptographische Hash-Funktion wird eine 256-bit Nonce mit einem Eingabewert verkettet. Von dieser Verkettung wird durch den Algorithmus ein Hash berechnet (Commitment). Nun kann nur durch Kenntnis von Nonce und Nachricht ein Rückschluss auf den Eingabewert gezogen werden, da eine Verifikation allen drei Parametern bedarf. Die Kollisionsresistenz beugt zusätzlich mehreren möglichen Lösungen vor.

2.2.4.3.3. Mathematische Aufgaben

Um eine effiziente Nutzung in einem System zu gewährleisten, müssen kryptographische Hash-Funktionen eine Freundlichkeit gegenüber mathematischen Aufgaben aufweisen. Bei einer mathematischen Aufgabe, oder einem mathematischen Problem handelt es sich in diesem Fall um eine Aufgabe, deren Lösungsfindung ein Durchsuchen eines großen Wertebereichs erfordert und bei welchem immer nur ein Lösungsweg existiert. Das Ergebnis dieser Aufgabe kann nur durch das Austesten von

zufälligen Werten (Noncen) gefunden werden. Bei einer 256-bit Funktion entspricht dies 2^{256} möglichen Ausgabewerten. Aus diesem Grund trägt die im Bitcoin-Netzwerk genutzte Hash-Funktion den Namen *SHA-256*.

2.2.4.3.4. SHA-256

Nachdem die theoretischen Eigenschaften von kryptographischen 256-bit Hash-Funktionen in den vorigen Kapiteln erläutert wurden, folgt nun eine genaue Betrachtung der von Bitcoin genutzten Hash-Funktion *SHA-256*. Diese besteht aus den Funktionen des *Merkle-Dåmgard-Verfahrens*[18], sowie einer *Kompressionsfunktion*. Diese Kombination bildet das Gerüst für die technische Funktionsweise der Blockchain.

Die Eingabewerte für SHA-256 resultieren aus dem Hash des vorigen Block-Headers[19], sowie den Hashs aller Transaktionen des neuen Blocks, auch bekannt als Transaktions-Identifikationsnummern (TXIDs). Die Anordnung dieser Hashs innerhalb des Blocks erfolgt in Form eines *Merkle Trees*. 1979 entwickelte der Schweizer Professor für Informatik Ralph Merkle Hash-Bäume als eine Hashlistenerweiterung, welche zur Unveränderlichkeit von Daten jeglicher Art beitragen. Wie in Abbildung 6 zu erkennen werden hierbei immer zwei TXIDs zusammengeführt und erneut gehasht. Anschließend werden aus den neuen Hashs weiterführend zwei dieser neuen Hash-Werte zusammengeführt und erneut gehasht. Dieser Prozess setzt sich fort, bis letztendlich ein finaler Hash Wert zustande kommt. Dieser einzelne Hash-Wert wird als *Merkle-Root* bezeichnet. Diese *Wurzel* des gesamten *Merkle* Baumes reflektiert alle Eingabewerte und lässt nachträglich die Richtigkeit dieser Informationen überprüfen.

[18] Eine Hash-Funktion, die einen beliebigen Eingabewert in einen Ausgabewert mit einer Größe von 512-bit umwandelt (ebd.).
[19] Der Blockheader stellte eine Zusammenfassung der Informationen eines Blocks dar (ebd.).

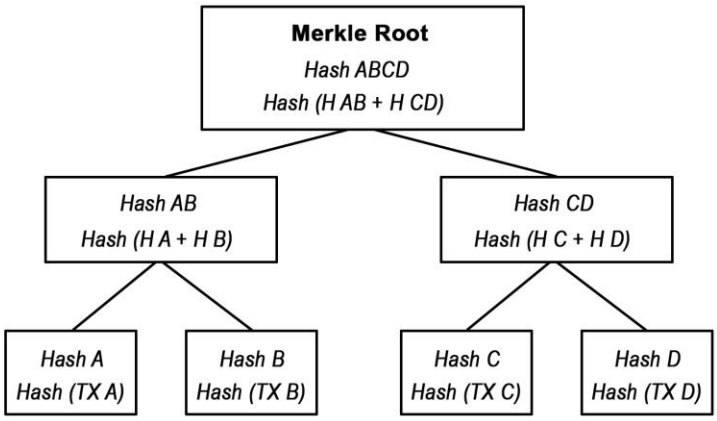

Abbildung 6: **Darstellung des Merkle-Trees.** Quelle: Eigene Abbildung, 2018.[20]

Bei SHA-256 wird der Eingabewert durch das Merkle-Verfahren in 512-bit große Blöcke aufgeteilt und anschließend mit dem Hashwert (256-bit) des vorigen Blocks der Kette verbunden. Hieraus resultiert eine Eingabegröße von 768-bit. Diese wird von einer Kompressionsfunktion auf 256-bit komprimiert und wiederum mit dem darauffolgenden 512-bit großen Block verbunden. Die Blöcke werden also komprimiert und anschließend doppelt verhasht. Dieser Prozess setzt sich durchgehend fort. Hierbei kommen auch sogenannte Hash-Pointer zum Einsatz, die in der Blockchain auf den Speicherort einer bestimmten Information verweisen und zwecks Verifikation der Gültigkeit einer Information auch die Hash-Werte beinhalten[21] (siehe Abbildung 7).

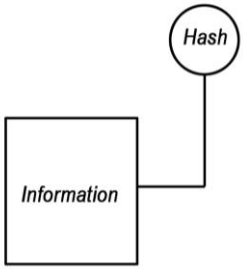

Abbildung 7: **Hash-Pointer.** Quelle: Eigene Abbildung, 2018

Diese Informationen bauen aufeinander auf und werden durch die Hash-Pointer verlinkt. Diese Liste aller Verlinkungen stellt die *Blockchain* dar. Durch das Miteinbeziehen des Hashs des letzten Blocks in den neuen Block kann durch die Hash-Pointer, neben dem Verweis auf die Daten, auch eine mögliche Fälschung nachgewiesen werden. Wie in Kapitel 2.2.4.3 beschrieben würde eine Änderung der Informationen eines vorigen Blocks den Ausgabewert des folgenden Hashs maßgeblich verändern, sodass das

[20] Eigene Darstellung in Anlehnung an Merkle, 1988, S. 293.
[21] Dies geschieht jedoch nur über die Daten selbst, um eine Nichtveränderung dieser nachweisen zu können. Ein Hash-Pointer verweist nicht physisch auf einen Speicherort (ebd.)

System durch diesen Rückschlüsse auf eine Manipulation ziehen kann. Der Hash-Pointer würde im Falle einer solchen Veränderung der Werte die neuen als *falsch* einstufen. Durch diese Methode kann also durch einen einzigen Block die gesamte vorangegangene Blockchain auf ihre Richtigkeit überprüft und Datenveränderungen aufgedeckt werden. Dieses Vorgehen erreicht die *Unveränderlichkeit* der Blockchain (siehe Abbildung 8).

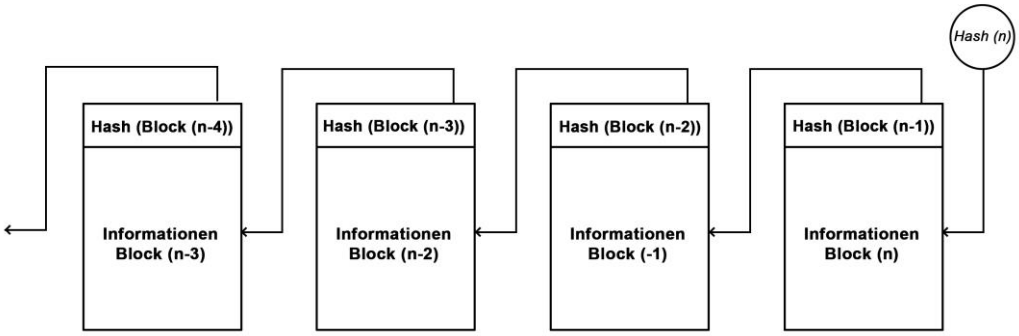

Abbildung 8: **Aufbau einer Blockchain.** Quelle: Eigene Abbildung, 2018.

2.2.4.4. Dezentralität des Netzwerks

Anschließend an die vorangegangene Darstellung der grundlegenden kryptographischen Funktionsweise der Blockchain folgt nun eine Analyse der Architektur des Bitcoin-Netzwerks zur Erreichung von Dezentralität. Der Autor definiert folgende Kriterien, um eine wissenschaftliche Beantwortung dieser Frage zu gewährleisten:

- Welche Systemeinheiten bewahren das Verzeichnis der Transaktionen?
- Welche Systemeinheiten verifizieren die Richtigkeit einer Transaktion?
- Auf welche Weise werden neue Bitcoin geschöpft?

2.2.4.4.1 Dezentrale Konsensfindung durch Nodes und Miner

Ziel der Dezentralisierung eines Systems ist es, die Gefahr eines Systemausfalls zu minimieren/eliminieren und somit dessen Zuverlässigkeit zu stärken. Dies stellt das System vor die Herausforderung, eine sichere und demokratisch synchronisierte Teilnahme durch dessen ausführende Mitglieder zu gewährleisten. Bei einem solchen Prozess der Teilnahme im System spricht man auch von Konsensfindung, da Regeln im System festlegen müssen, auf welche Weise die Einheiten miteinander kommunizieren und Einigkeit in ihrem Wirken erreichen. Auch muss gewährleistet sein, wie ehrliche Nodes von den fehlerhaften oder böswilligen unterschieden werden und diese abgelehnt werden können. Ebenso gelten Regeln für die Miner, die die Transaktionen verarbeiten und über das System selbst belohnt werden. Der technische Prozess wird folgend dargelegt:

Entgegen einer oft fälschlichen Darstellung besteht ein Unterschied zwischen Minern und Nodes. Bei den Nodes wird zwischen *Full-* und *Light-Nodes* unterschieden. Unter Full-Nodes werden die bisher der Verständlichkeit wegen nur als Nodes beschriebenen Einheiten bezeichnet, welche einzig und allein zur Speicherung[22] der Blockchain und zur Verifizierung der Transaktionen in den Blöcken, sowie zur Überwachung der Miner existieren. Diese werden non-profit von privaten Individuen/Gruppen oder Organisationen betrieben, die dies aus verschiedenen ideologischen oder weiteren nicht wirtschaftlichen Gründen tun. Zum Zeitpunkt dieser Arbeit agieren 11605 Full-Nodes im Netzwerk, verteilt über die gesamte Welt mit großer Konzentration in den westlichen Staaten (Bitnodes, 2018). Bei Light-Nodes handelt es sich hingegen nur um Schnittstellen zur Blockchain, die das Kommunizieren und Scannen der Transaktionen in der Blockchain übernehmen. *Wallets*[23] fungieren als Light-Nodes und kommunizieren neben dem Halten der Keys auch die Transaktionen in das Netzwerk. Des Weiteren beobachten sie diese und achten auf Transaktionen, die an eigens gehaltene Public-Keys adressiert sind, um einen Werteingang festzustellen. Wallets werden dabei neben der offiziellen Software des Hauptentwickler-Teams auch von Drittanbietern bereitgestellt, welche in vielen Fällen neben Bitcoin-Schlüsselpaaren auch das Halten der Keys weiterer Krypto-Assets erlauben (Kapitel 2.2.4.2).

Bei Minern handelt es sich hingegen um Unternehmen oder Individuen, die dem System ihre Rechenleistung aus wirtschaftlichen Gründen bereitstellen. Hierbei sind drei Elemente erforderlich: Spezialisierte Hardware, schneller Internetzugang und Strom.
Miner wandeln dabei Energie in Systemsicherheit um, da sie die Aufgabe der Sammlung und Gruppierung, sowie Verhashung der Transkationen übernehmen. Bei diesem Sicherheitskonzept spricht man von Proof-of-Work (PoW). Dieses ist extrinsisch, da Energie außerhalb des Systems verpflichtet wird. Bricht jemand die Regeln, hat er die gesamte Energie, die er aufgewendet hat, verschwendet. Durch die aufgewendete Arbeit lässt sich ein hohes Level an Unveränderlichkeit erreichen. Diese Erreichung wird auch als *Historical Record Keeping* beschrieben. Um einen Block auf der Blockchain zu verändern, bedarf es der erneuten Rechenleistung, die zur Erstellung dessen und aller davor gelegenen Blöcke im System notwendig war. Das bedeutet, dass für jeden Block die gleiche Menge an Rechenleistung und Stromverbrauch aufgebracht werden muss, um diese zu verändern. Aus diesem Grund ist es praktisch extrem schwer etwas, das auf der Blockchain durch PoW eingetragen wurde, zu verändern. Aktuell verbraucht das Netzwerk zwischen 500 Megawatt und einem Gigawatt an Elektrizität pro

[22] Die Datengröße der Blockchain beträgt 137 Gigabyte (Blockchain.info, 2018)
[23] Unter Wallets werden Programme oder Hardware verstanden, die einen Zugriff auf die Blockchain, zwecks lesen und kommunizieren, ermöglichen (Kapitel 2.2.4.2.)

Tag. Um also die Transkationen des letzten Tages rückwirkend zu verändern, was ungefähr 144 Blöcken entspricht, benötigt man dementsprechend 1.2 Gigawattstunden in Elektrizität. Dieser unglaubliche Energieaufwand wäre für eine böswillige Entität nicht einmal ansatzweise wirtschaftlich, falls technisch überhaupt zu bewerkstelligen. Das Minen findet jedoch überwiegend in *Mining-Pools* statt. Bei diesen kann sich jeder Miner weltweit in das Mining-Netzwerk einklinken und seine Rechenleistung bereitstellen. Die geschöpften Bitcoins werden dann täglich, entsprechend der prozentual im System eingesetzten Rechenleistung, an die Miner verteilt. Diese Menge der verschiedenen Pools hat sich in den letzten Jahren nach und nach reduziert. Stand 05.01.2018 existieren sieben, die zusammen über 73% der Hash-Power, also der bereitgestellten Rechenleistung ausmachen.
Das Proof-of-Work System nimmt enorme Mengen an Energie in Anspruch. Setzt man diese jedoch ins Verhältnis zu den Stromkosten einer Bank, bei welcher riesige Serverstrukturen für Sicherheit, Transaktionen und Datenspeicherung, diverse Bankautomaten, sowie weitere Unmengen an Stromkosten für weitere Zahlungsdienste aufgebracht werden, so wird davon ausgegangen, dass Bitcoin im Vergleich ähnliche und nicht höhere Stromkosten verursacht (Platzer, 2016).

2.2.4.4.2. Transaktionsverlauf

Im Folgenden wird der Verlauf einer Transaktion im System dargelegt, um darauf aufbauend weitere Chancen und Risiken dieses Netzwerks, in Bezug auf die Nutzung als Tausch-und Zahlungsmittel, zu ermitteln.

Wird eine Transaktion von einer Full-Node oder der Lightnode eines Wallets in das Netzwerk gesendet, so wird diese Transaktion an alle Miner kommuniziert. Aufgrund der Datenübertragungsgeschwindigkeit erreichen diese Transaktionen geographisch betrachtet, durch die Distanz zu diesen, einige Miner an näheren Standorten früher, andere später. Miner sammeln durchgehend über einen Zeitraum von 10 Minuten unabhängig voneinander Transaktionen. Dabei bestimmen sie ihre eigene Auswahl, welche sie in einen Block gruppieren, bis 1MB Datengröße annähernd erreicht ist. Zusätzlich inkludieren sie eine gewisse Anzahl von Bitcoins, die bisher in dem Verzeichnis nicht verzeichnet sind (siehe Abbildung 9). Die Höhe dieses Wertes halbiert sich, sobald eine bestimmte Blockanzahl im System erreicht ist (alle vier Jahre). Dies führt sich fort bis 21 Millionen Bitcoin geschöpft wurden.

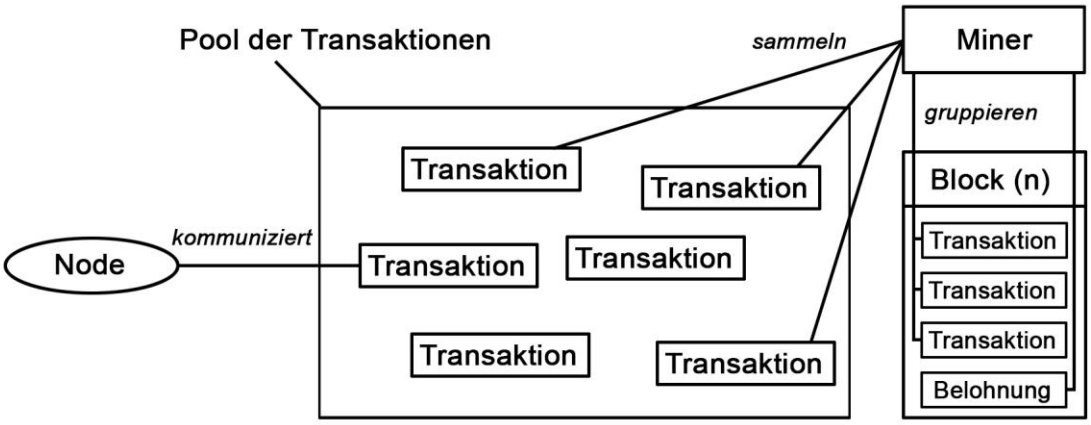

Abbildung 9: **Technische Arbeitsweise der Miner.** Quelle: Eigene Abbildung, 2018.

Dadurch kreiert der Miner neue Bitcoins und "schöpft" diese aus dem Nichts. Auf diese Weise erhalten die Miner neben *Transaktionsgebühren* ein Incentive (*Block-Reward*), um ihre Rechenleistung für die Gruppierung der Transaktionen bereitzustellen. Diese dürfen jedoch erst nach 100 Bestätigungen von Nodes auch ausgegeben werden (Öndner, Tucci, Piergiovanni & Pozzo, 2017, S. 12 ff). Aktuell achten die Miner dabei jedoch auch auf die Höhe der Transaktionsgebühren, die die Nutzer von Bitcoins beim Versenden einstellen können. Transaktionen mit höheren Gebühren werden dabei von den Minern bevorzugt. Viele Schnittstellen, wie Wallets oder eigene Nodes lassen den Nutzer die Gebühren je nach Bedarf justieren. Die überwiegende Anzahl der Börsen, sowie einige Wallets verwehren dem Nutzer jedoch diese Freiheit und stellen automatisch eine Gebühr ein, die sich nach dem jeweiligen Transaktionsaufkommen der bisher unbestätigten Transaktionen richtet, um sicherzugehen, dass die Miner die gewünschte Transaktion bevorzugen und möglichst schnell in ihre Blöcke mitaufnehmen.

Anschließend versuchen die Miner eine, in Kapitel 2.2.4.3.3 beschriebene, mathematische Aufgabe zu lösen, deren Eigenschaft darauf beruht, dass der Computer eine zufällige Lösung erraten muss. Das Ziel hierbei ist es, eine bestimmte Anzahl der Zahl 0 am Anfang des Hashs zu erhalten, die das System vorgesehen hat. Der Miner probiert also durchgehend verschiedene Noncen aus, um die richtige Antwort zu erhalten (Kapitel 2.2.3.5.). Ist diese Anzahl erreicht, so ist die Antwort valide und der ausführende Miner erhält die Erlaubnis, den Block an das Netzwerk zu kommunizieren. Alle Nodes empfangen und überprüfen anschließend diesen Block und fügen diesen, wie in Abbildung 10 zu erkennen, in ihre Blockchain ein. So erhalten alle immer das gleiche Verzeichnis.

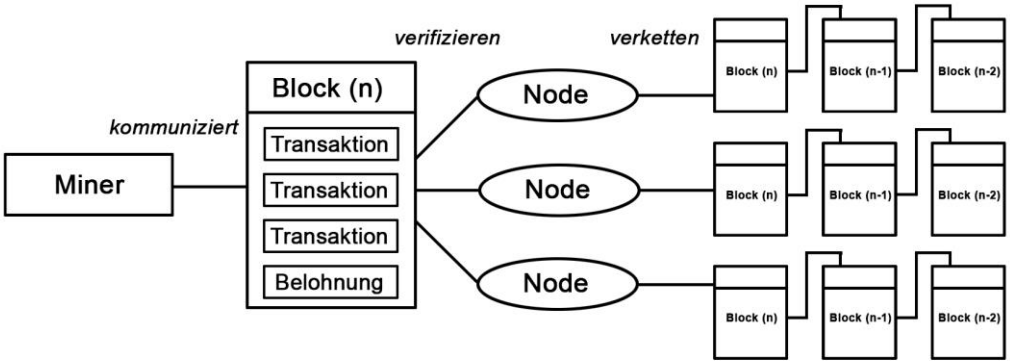

Abbildung 10: **Verifikation und Verkettung durch die Miner.** Quelle: Eigene Abbildung, 2018.

Die Überprüfung des Blocks und dessen Lösung kann leicht durchgeführt werden. Hierbei fügen die Nodes nur die Hashs der Transaktionen, sowie der zum Erfolg beigetragenen Nonce in die Hashfunktion. Erhalten sie den gleichen Wert, gilt die Transaktion als valide. Dabei definiert das Mehrheitsprinzip was als richtig, und was als falsch gilt. Wenn über 50% der Nodes eine gleiche Aussage treffen, gilt diese als valide. Im Falle einer annähernd gleichzeitigen Lösungsfindung achten die Nodes auf die Zeitstempel der gelösten Aufgabe. Dem Miner, der den richtigen Hash zuerst gefunden hat, wird die Belohnung zugesprochen. Zusätzlich folgen die Nodes immer der längsten Kette. Durch die Größe des Systems, in dem jeder versucht, diese Lösung zu erraten, wird einer der Miner diese in der vorhergesehenen Zeit von 10 Minuten finden. Hierbei passt das System den Schwierigkeitsgrad dieser Rechenaufgabe an die Anzahl die aktiven Miner alle zwei Wochen an, wodurch die Geschwindigkeit der Bearbeitung der Transaktionen immer gleichbleibt. Durch dieses Zufallsprinzip wird einem möglichen Betrug vorgebeugt, da niemand vorhersehen kann, welcher Miner die richtige Lösung erhält.

2.2.4.4.3. Systemimmanente Skalierungsprobleme

Aufgrund der beschriebenen Zeit von 10 Minuten, nach denen jeweils ein Block mit einer Größe vom maximal 1MB in die Blockchain eingefügt werden darf, kommt es bei großen Transaktionsmengen zu langen Wartezeiten. Die vom System vorgeschriebenen 10 Minuten sind dabei auf die Sicherheit des Netzwerks zurückzuführen. Dieses verteilt sich über die gesamte Welt und die Dauer zwischen dem Verkünden eines Blocks benötigt daher genügend Zeit, damit alle Nodes diesen rechtzeitig erhalten, verifizieren und einfügen können. Würde die mögliche Blockgröße erhöht oder die Zeit verringert werden, so stiege damit exponentiell die benötigte Rechenleistung der Miner und Nodes, sowie der benötigte Bedarf an Datenübertragungsgeschwindigkeit/Datenmenge des Internets. Durch diese ansteigenden Anforderungen würde das Betreiben von Nodes den meisten privaten Individuen fortschreitend

unmöglich machen, da die Kosten ebenfalls exponentiell ansteigen, was ebenfalls für die Miner gilt. Sollten die Netzwerkeintrittsbarrieren erhöht werden, wäre das Ergebnis eine mehr und mehr zentralisiertere Version Bitcoins, wodurch dies den Gefahren der Zensur und weiterer Angriffe ausgesetzt würde. Zum Zeitpunkt der Veröffentlichung dieser Arbeit (02.02.2018) ist keine technische Lösung für eine grenzenlose Skalierung der Blockchain bekannt. Lediglich die Nutzung von zentralen Zahlungskanälen stellt eine theoretische Lösung dar, die jedoch noch nicht final entwickelt und getestet wurden. Die am weitesten fortgeschrittene Entwicklung stellt dabei das *Lightning-Network*[24] dar. Eine Nutzung würde jedoch die Inanspruchnahme eines zentralisierten Services (Drittanbieter) bedeuten, welcher zusätzlich in den Systemen der Sender und Empfänger integriert werden muss.

2.2.4.4.4 Double-Spend-Attacke

Die Funktionsweise der Blockchain beugt auch, wie in Kapitel 2.2.2 beschrieben, dem doppelten Ausgeben von Bitcoin vor. Würde ein Nutzer eine Transaktion im System doppelt einreichen, und ein Miner diese aufnehmen, so würde nur die erste gültige gezählt werden. Dies wird auch anhand von Zeitstempeln überprüft. Die weitere Transaktion wird als falsch identifiziert. Würden beide Transaktionen jedoch simultan von zwei verschiedenen Minern aufgenommen, und in ihren jeweiligen Block eingepflegt werden, so würden die Nodes diese anfangs als valide identifizieren. Das Protokoll der Nodes sieht jedoch vor, dass immer der längsten Blockchain gefolgt wird. Erreicht ein Block Bestätigungen von sechs oder mehr Nodes, die diesen in ihr Verzeichnis eintragen, so gilt dieser als unveränderbar. Der Block, der diese sechs Bestätigungen zuerst erreicht, wird also als valide erklärt, der weitere als falsch. Die Nodes, die den falschen in ihrem System eingetragen haben, stoppen in diesem Fall ihre Arbeit an der bisherigen Kette und arbeiten mit der validen Blockchain weiter. Der Versuch Bitcoin doppelt auszugeben ist also nicht möglich.

Eine doppelte Ausgabe der Bitcoin wäre jedoch unter Umständen durch eine 51%-Attacke möglich. Hierfür müsste eine böswillige Entität über 51% der gesamten Rechenleistung des Systems aufbringen, was in keinem wirtschaftlichen Verhältnis stehen würde. Selbst wenn es gelingen würden, alle Teilnehmer der großen Miningpools zusammenzuschließen, wobei es sich um mehrere 100.000 bis mehrere Millionen handeln würde, so hätten diese zwar die Kapazität, um eine solche Attacke

[24] Bei dem Lightning-Network kommunizieren die jeweiligen Transaktionspartner die Transaktion(en) abseits der Blockchain Bitcoins in einem separaten Kanal. Die Zahlungsvorgänge werden anschließend zusammengefasst an das Bitcoin-Netzwerk kommuniziert. Eine Nutzung dieser Möglichkeit eliminiert damit die Transaktionskosten und senkt die Zeiten auf ein Minimum.

durchzuführen, der wirtschaftliche Anreiz wäre jedoch sehr gering, da der Besitz von über 50% der Rechenleistung durch das Netzwerk weitaus mehr einbringen würde.

2.2.4.4.5. Hard Forks

Für die Weiterentwicklung der Software sind die Entwickler des Bitcoins (BTC) zuständig, die auch als Bitcoin-Core Team bezeichnet werden. Diese arbeiten fortlaufend an dem Code und führen Verbesserungen durch. Da das Blockchain Netzwerk keiner zentralen Autorität gehört, können Änderungen an der Software nicht ohne die Zustimmung der Mehrheit vorgenommen werden. Dies erfolgt über eine demokratische Abstimmung. Diese Art der Konfiguration eines besitzerlosen Systems erzeugt eine höhere Sicherheit und beugt Täuschungsversuchen vor, da die Software zuvor inspiziert und deren Vor- und Nachteile diskutiert und abgewogen werden können. Dennoch ist dieser kleine und elitäre Kreis der Entwickler maßgeblich für die Entwicklung des Bitcoins zuständig, was eine Fragilität des Ökosystems nicht ausschließt.
Sind einige Shareholder/Stakeholder des Systems jedoch nicht mit der Entwicklung des Core-Teams einverstanden, so können sie die Open-Source Software nach ihrem Belieben weiterentwickeln und dies an die Community kommunizieren, in der Hoffnung, dass die Miner und Nodes die neue Software akzeptieren. Dies geschieht über sogenannte *Hard Forks*, bei denen das aktuelle Verzeichnis nach der Änderung sowohl auf der alten, als auch auf der neuen Blockchain getrennt fortgeführt wird. Dabei gilt es die Besitzer der Nodes von der neuen Version der Blockchain zu überzeugen, die diese dann auf den Computern installieren müssen. Eine Hard-Fork des Netzwerks bedarf also eines politischen Prozesses, bestehend aus Überzeugung und Transparenz. Anschließend koexistieren diese Systeme und die Nutzer, die vor der Fork Bitcoins im Verzeichnis hatten, besitzen nun auf beiden Verzeichnissen die gleiche Anzahl an Coins. Je nach Marktwert erhalten diese somit zusätzlichen Wert. Da die neu *geforkten* Coins jedoch oft Bitcoin im Namen tragen, die bekannteste Fork hierbei ist BitcoinCash, führt dies am Markt oft zu Verwirrung und Diskussion. Hierbei entscheidet auf lange Sicht der Markt, welche Version er bevorzugt, oder ob beide genutzt werden sollen (Dreschner, 2017, S.32-34).

2.2.5. Nutzung als Tausch- und Zahlungsmittel

In den vorigen Kapiteln wurden nun die technischen Eigenschaften und Funktionsweisen des Bitcoin-Systems analysiert. Dabei lassen sich diese wie folgt zusammenfassen:

1. Peer to Peer - direkt und ohne Mittelsmann
2. Dezentral (Robust) - kein *Single Point of Failure* bei Ausfall einer oder mehrerer Teilnehmer des Netzwerks

3. Kein Vertrauen benötigt - Alle Aktivitäten sind transparent, nachvollziehbar und überprüfbar
4. Hohe Systemsicherheit durch Kryptographie
5. Unveränderlich - Eine eingetragene und verifizierte Änderung kann nicht mehr abgeändert werden
6. Mathematisches Protokoll der Endlichkeit erreicht deflationäre Eigenschaften
7. System hält sich selbst durch Miner und Nodes aufrecht (Gelschöpfung durch System selbst)
8. Änderungen oder Abspaltungen erfolgen demokratisch und werden durch den Markt geregelt

Diese Eigenschaften[25] stellen die zentralen Aspekte dar, um die Chancen und Risiken von Bitcoin als Tausch-und Zahlungsmittel zu überprüfen. Damit sich Chancen in der Nutzung von Bitcoin als solches ergeben, müssen die Eigenschaften des Systems und dessen Nutzbarkeit effizient und ökonomisch, sowie einfach anwendbar sein. Das folgende Kapitel untersucht in diesem Zuge weiterführend die ökonomische Effizienz der Nutzung von Bitcoin als Zahlungsmittel, sowie die Usability der Transaktionsmedien (Wallets).

2.2.4.1 Ökonomische Effizienz

Trotz der Eliminierung von Intermediären, entstehen in dem Bitcoinnetzwerk sehr hohe Transaktionskosten. Diese schwanken zwischen 20$ und 50$ und greifen bei jeder Transaktion (Bitinfo 2018)[26]. Dies ist auf die in Kapitel 2.2.3.5 beschriebene Blockgröße und Findungszeit zurückzuführen. Aus dem Grund, dass nur alle 10 Minuten ein Block in die Blockchain eingetragen werden darf, welcher eine maximale Größe von 1MB besitzt, kann das Netzwerk bei steigender Nutzerzahl nicht unendlich skalieren und stößt an seine Grenzen. Die gewählte Zeit von 10 Minuten gibt allen Nodes im System zwar genügend Zeit, das Verzeichnis synchron zu halten, verhindert jedoch, dass Blöcke öfter eingefügt werden können. Dies führt zu einem Flaschenhalseffekt, da ein Block nur ungefähr 2000 Transaktionen beinhalten kann und dennoch durchschnittlich 150.000 Transaktionen im Pool der wartenden Transaktionen auf eine Verarbeitung warten. Zusätzlich zu dem Anstieg der Transaktionskosten kommt hinzu, dass die Miner sich die Transaktionen aussuchen, die mit den höchsten Transaktionsgebühren versehen werden. Je mehr der Nutzer zahlt, desto schneller wird seine Transaktion also in einen Block aufgenommen. Wird Bitcoin also als Zahlungsmittel verwendet,

[25] ([in chronologischer Reihenfolge] Steinmetz, 2004, S. 51-54; Morabito, 2017, S. 23-26; Dannen, 2017, S. 2 ff; Diffie & Hellmann, 1976, S. 646; ebd.; Morabito, 2017, S. 32)
[26] Der untersuchte Zeitraum der Transaktionskosten: 01.10.2017-15.01.2018 (Bitinfo, 2018).

fallen bei jeder Transaktion eben diese Gebühren an. Dies ist als nicht wirtschaftlich zu erachten und nur bei sehr hohen Zahlungen in Betracht zu ziehen.

2.2.4.2 Nutzung von Wallets als Zahlungsmedium

Die Systemeigenschaft der transparenten Anonymität[27] setzt eine korrekte Eingabe der Public-Keys bei der Durchführung einer Transaktion voraus. Da diese jedoch keiner Person namentlich zugeordnet werden bedeutet ein Tippfehler in der Adresse das Senden an eine ungewollte. Dies ist nicht umkehrbar und hat den Verlust der gesamten Bitcoins zur Folge. Diese Unumkehrbarkeit der Transaktionen birgt also das Risiko, anfällig für menschliche Fehler zu sein. Zum Zeitpunkt der Veröffentlichung dieser Arbeit[28] weisen die Wallets keine hohe Usability auf. Beispielsweise fehlt die Funktion einer Adressspeicherung oder der Überprüfung der Richtigkeit der Adresse.[29]

2.3. Zentrale Geldsysteme und Währungen

Das folgende Kapitel befasst sich mit der Analyse von Geld und Währungen, sowie der Funktionsweise des Bankensystems und möglicher Zahlungsmittel. Dies ist erforderlich, um Bitcoin in den Marktkontext einzuordnen und entsprechende Chancen und/oder Risiken in der Nutzung als Tausch-und Zahlungsmittel zu identifizieren. Aus diesem Grund bedarf es eben dieses Vergleichs mit den bisher konkurrenzlosen und zentral gesteuerten herkömmlichen Tausch-und Zahlungsmitteln am Markt, den Währungen. Der Autor weist an dieser Stelle daraufhin, dass eine umfassende Analyse aller staatlichen Währungen und am Markt bestehenden Zahlungssysteme, mit denen Bitcoin direkt und indirekt konkurriert, den Rahmen dieser Arbeit weit übersteigen würde. Aus diesem Grund werden Währungen im Allgemeinen behandelt, mit Fokus zwecks Erklärungsvereinfachung auf dem Euro, sowie herkömmliche Zahlungsmethoden am Markt übergreifend betrachtet. Um Bitcoin in diesem Kontext zu vergleichen und dessen Chancen und Risiken durch den Einfluss zentraler Währungen und deren nutzbarer Zahlungsmethoden zu ermitteln, definiert der Autor folgende Fragen, die der wissenschaftlichen Beantwortung der Leitfrage dienlich sind:

- Welche Eigenschaften liegen Geld zugrunde?
- Was unterscheidet Geld von einer Währung?
- Ist Bitcoin als Geld und/oder Währung zu definieren?

---

[27] Alle Transaktionen sind auf der Blockchain nachvollziehbar, bekannt sind jedoch nur die Public-Keys, welche keine Rückschlüsse auf den Besitzer ziehen lassen.
[28] Stand 02.02.2018
[29] Der Autor hat die folgenden, gängigen Wallets betrachtet: Softwarewallets - Electrum, Exodus, Core-Wallet (Full-Node), Hardwarewallet - Ledger Nano S. Dabei ist darauf hinzuweisen, dass weitere Wallets am Markt nach Kenntnisstand keine weiteren Funktionen aufweisen als die getesteten.

- Welche Systeme liegen Währungen zugrunde?
- Welche Auswirkungen haben die systemimmanenten Eigenschaften von Währungen auf die Nutzung dieser als Zahlungsmittel?
- Welche Eigenschaften haben herkömmliche Zahlungsmittel?

2.3.1. Geld und Währung

2.3.1.1. Geldeinheiten als Tausch- und Zahlungsmittel

Geld ist als indirektes Tauschmittel zu definieren. Es schafft, mittels der ihm immanenten Kaufkraft, Abhilfe für einen direkten bilateralen Naturalaustausch, also einen Austausch, bei dem beide Partner gleichzeitig Bedarf an den Realgütern des anderen mit ähnlichem Gegenwert haben. Folglich ermöglicht Geld zwei einseitige Momente des Kaufs und Verkaufs (Wildmann, 2007, S. 105). In der Betriebswirtschaft spricht man dabei von einer zeitlichen Trennung dieser beiden Tauschvorgänge (Plassaras, 2013, S. 19). Weiterführend wird die Ebene der räumlichen Trennung durch das Buchgeld erreicht. Buchgeld oder auch Giralgeld, entsteht durch die Einzahlung von Geld auf die für den Zahlungsverkehr benötigten Banknoten, mit deren Hilfe eine Überweisung getätigt werden kann. Da der Prozess einer Überweisung nicht die Anwesenheit beider Tauschpartner erfordert, wird hierbei von einer räumlichen Trennung gesprochen. Der Bielefelder Soziologe Niklas Luhmann betrachtet die Wirtschaft als autopoietisches System, in welchem Zahlungen durch Zahlungen ermöglicht werden und sieht Geld dabei als „symbolisch generalisiertes Kommunikationsmedium der Wirtschaft“ (1984), da es ohne Materialwert nur durch seine allgemeine Anerkennung und Akzeptanz als Mittel zur Verständigung seinen Wert erhält. Das Vertrauen in das vorherrschende Geldsystem ist dabei unumgänglich. Andernfalls hätte die Währung einzig ihren Materialwert, der abgesehen von Münzgeld in den meisten Fällen gegen null geht.

Als volkswirtschaftliches Organisationsmittel erfüllt Geld neben dem Nutzen als Tausch- und Zahlungsmittel dabei zwei weitere maßgebliche Funktionen: Recheneinheit und Wertaufbewahrungsmittel.

2.3.1.2. Geldeinheiten als bevorzugte Recheneinheit

Um eine Vergleichbarkeit der Wertigkeiten verschiedener Güter herbeizuführen, können Geldeinheiten als gemeinsamer Maßstab genutzt werden. Kostet eine Hose beispielsweise 60€, so hat diese den gleichen Wert wie etwa vier Kinobesuche a 15€. Die Notwenigkeit dieser Vergleichbarkeit zeigt sich vor allem beim Handel im Ausland. Unterschiedliche Kurse unterschiedlicher Währungen kreieren unterschiedliche Kosten für das gleiche Produkt. Des Weiteren erleichtert Geld in dieser Funktion diverse Aufgaben, die bei der Führung von Wirtschaftseinheiten, wie Haushalten oder

Unternehmen, anfallen (Stocker, 2006, S. 49). Eine Nutzung von Geldeinheiten als Recheneinheit bedeutet daher in vielen Fällen eine relevante Zeitersparnis.

2.3.1.3. Geldeinheiten als Wertaufbewahrungsmittel

Da Geld in einem System beim Kauf und Verkauf von Gütern das bevorzugte Zahlungsmittel darstellt, erlaubt dessen Besitz eine Speicherung des Wertes auf Zeit, vorausgesetzt das Vertrauen in diesem Zeitraum bleibt bestehen, um eine Wertstabilität zu garantieren. Durch diese bereits erwähnte inhärente Kaufkraft des Geldes, kann dieses die Funktion eines Tauschmittels auch zukünftig erfüllen. Folglich ermöglicht Geld den Tauschpartnern eine Zeitüberbrückung zwischen dem Verkauf und dem Kauf von Gütern, sowie umgekehrt. Geld ist auch als Mittel der Vermögensbildung zu sehen (Kiyotaki & Wright, 1989, S. 927-954). Als liquidestes Mittel für diesen Zweck hat es dabei allerdings den Nachteil, dass Bargeld nicht und Buchgeld nur sehr gering verzinst wird. Weiterhin ist Bargeld der Gefahr einer Entwertung im Falle einer Inflation ausgesetzt. Dies birgt Kosten und Risiken.

2.3.1.4. Unterschied Geld und Währung

Der Unterschied zwischen den genannten Begriffen liegt einzig und allein in der wirtschaftlichen Einbindung des Mediums. Geld gilt als Währung, wenn es das meist akzeptierte Zahlungsmittel innerhalb eines geographischen Raumes darstellt, welches auch als offizielles Mittel der Steuerabgabe an den Staat verwendet wird (Wildmann, 2007, S. 177ff). Dabei können die genutzten Einheiten einer Währung auch als Geldeinheiten bezeichnet werden. Bezogen auf die wichtige Funktion als Wertaufbewahrungsmittel, zeigt der geschichtliche Hintergrund von Währungen dabei: Das Halten dieser beruht immer auf dem Vertrauen und der Erwartung, dass der monetäre Wert sich über einen absehbaren Zeitraum insofern nicht verändert, dass das Geld merkbar an Wert verliert (Wildmann, 2007, S.201). Ist die Währung nicht an einen Rohstoff wie Gold gebunden, so ist das Vertrauen in das System und dessen Verwalter unabdingbar.

2.3.1.5. Ausprägungen von Währungen

Es existieren unterschiedliche Formen von Währungen. Diese lassen sich in zwei Oberkategorien aufteilen, die des physischen, und die des elektronischen Geldes. Physisches Geld umfasst Warengeld, Banknoten (Papiergeld), Münzen und Buchgeld (Giralgeld). Sowohl Münzen, als auch Papiergeld werden als Bargeld bezeichnet. Unter der Kategorie "Kreditgeld" oder auch "stoffwertloses Geld", ordnet man dabei Banknoten und Buchgeld ein. Kreditgeld wird als solches bezeichnet, da der Verkäufer eines realen Wertes, wie zum Beispiel einer Ware, ein schriftliches Versprechen in

Form des Geldes erhält, welches wiederum erneut einen temporär versetzten Bezug eines realen Wertes ermöglicht (Wildmann, 2007, S. 107 ff). Dieses Geld stellt für den Ausgebenden (z.B. die Notenbank) eine Verbindlichkeit dar. Der Begriff stoffwertlos wird dabei aufgrund des unbedeutenden Eigenwertes des Geldes, also dessen Materialwert, verwendet. Das Buchgeld liegt hingegen nicht als Bargeld, sondern als sofort liquidierbares Guthaben auf einem der Konto der ausgebenden Entität vor.
In der Kategorie des elektronischen Geldes lassen sich Einlagen von finanziellen Instituten in der Zentralbank (Zentralbankdeposite) und Einlagen von Haushalten und Unternehmen in kommerziellen Banken (Kommerzielles Bankengeld) identifizieren (Tarkka, 1995, S.15-19). Diese Geldeinheiten liegen auf den Speichermedien der Banken in Form von BIT-Einheiten (Datenpaketen) vor, welche zwischen den Computern der Akteure der Wirtschaft hin-und herwechseln.

2.3.2. Bitcoin als Krypto-Asset

Im Folgenden werden nun die Eigenschaften einer Währung mit denen Bitcoins verglichen um festzustellen, ob das Medium definitorisch als Währung identifiziert werden kann.
Das erste Merkmal einer Geldeinheit und einer Währung, Tausch-und Zahlungsmittel darzustellen ist bei Bitcoin überwiegend gegeben. Die technische Architektur erlaubt es, Bitcoin als Tausch- und Zahlungsmittel zu nutzen, obgleich dieses am Markt bisher wenig Akzeptanz als solches gefunden hat (Chokun, 2018). Als Recheneinheit ist Bitcoin nur bedingt anzusehen, da es zwar mathematisch teilbar, aufgrund der Schwankungen am Markt jedoch schwer als Vergleichseinheit zu Produkten wie einem Brot beim Bäcker genutzt werden kann. Der Aspekt der Wertspeicherung ist aufgrund der deflationären Eigenschaften des Mediums, nur bedingt gegeben. Der Wert des Bitcoin ist sehr volatil und nimmt auf lange Sicht stetig zu, weswegen es schwer vorherzusehen ist, wie viel die gehaltene Anzahl auf lange Zeit wert ist. Wertspeicherung bezieht sich überwiegend auf eine absehbare *Nichtveränderung* des Wertes auf Zeit, sprich *Speicherung* und nicht *Vermehrung/Verminderung* (Wildmann, 2007, S. 104 ff). Vor allem aber der Aspekt, dass eine Währung die in einem bestimmten geographischen Raum, meist akzeptierte Zahlungseinheit ist, trifft auf Bitcoin nicht zu. Nur vereinzelte Firmen bieten die Zahlung mit Bitcoin an, viele dieser, wie Microsoft und Steam, haben diese Zahlungsmethode jedoch wieder abgeschafft, da Volatilität und Transaktionskosten des Mediums zu unvorhersehbar und zu hoch sind (Valve Corporation, 2017; Cimpanu, 2018).
Unter der Berücksichtigung der identifizierten definitorischen Merkmale einer Währung, ist Bitcoin somit unter den genannten Aspekten nicht eindeutig als Währung zu definieren, obgleich dessen Eigenschaften Ähnlichkeiten aufweisen. Dieses neuartige

Medium besitzt neben den Ähnlichkeiten mit einer Währung auch weitere verschiedene Charakteristika, die *Assets* aufgrund der Volatilität und der Preisgestaltung am Markt Rohstoffen und Aktien ähneln. Aus diesem Grund verwendet der Autor hierbei den Begriff *Asset* (Knolle-Grothusen, 2009, S. 131 ff). Bei einem Asset handelt es sich um ein Gut mit wirtschaftlichem Nutzen (Gabler, 2013). Aufgrund der genannten Charakteristika vieler Eigenschaften, kommt zusätzlich das Adjektiv *hybrid* zum Tragen. Die Definition des Bitcoin als hybrides Krypto-Asset umfasst damit alle Eigenschaften des Krypto-Mediums und wird diesem gerecht. Der Autor weist an dieser Stelle daraufhin, dass die starken Ähnlichkeiten mit einer Währung, trotz einer nicht möglichen Definition als solche, dennoch einen wissenschaftlichen Vergleich im Hinblick auf die Beantwortung der Forschungsfrage, zulassen.

2.3.3. Zentralbanken

Bei den Herausgebern von Währungseinheiten handelt es sich in den meisten Fällen um den jeweiligen Staat, in vereinzelten Fällen auch um private Organisationen[30]. Der Autor bezieht sich in der folgenden Erklärung der Aufgaben einer Zentralbank überwiegend auf die Europäische Zentralbank (EZB). Verschiedene Zentralbanken verschiedener Länder haben einen ähnlichen Aufbau, verfolgen jedoch oft unterschiedliche Ziele. Eine Betrachtung aller Zentralbanken der Welt würde dabei den Umfang dieser Arbeit weit übersteigen. Aus diesem Grund wird das Modell einer Zentralbank an dem genannten Beispiel theoretisch dargelegt.

Hauptaufgaben einer Zentralbank (ZB) stellen die Ausgabe von Geld, die Verwaltung von Währungsreserven, Sicherung der Stabilität der Währung im äußeren Raum, sowie die Herstellung von Preisniveaustabilität[31] im inneren Raum dar (Wildmann, 2010, S. 64). Um letztere zu erreichen nutzt die ZB das Instrument der Geldmengensteuerung. Hierbei handelt es sich um die Kontrolle der Geldmenge über das Drucken von neuem Geld. Da eine Zentralbank die Geldmenge jedoch nur vermehren und nicht verknappen kann, spricht man dementsprechend von einem inflationären System (Wallace, 2014, S. 259-274). Dieser Vorgang geschieht nicht nur in Form von physischen Banknoten, welche bei Geschäftsvorgängen mit hohen Summen eine immer geringere Rolle spielen, sondern auch als BIT-Einheiten (Bheemaiah, 2017, S. 126 ff; Kapitel 2.3.1). Diese Steuerung der Geldmenge wird von einer Zentralbank als

[30] In den USA gibt die Federal Reserve Bank (FED) die Banknoten heraus und verwaltet diese. Bei der FED handelt es sich um eine private Notenbank, die nach der großen Wirtschaftskrise 1913 mit dem Ziel einer sicheren Kreditbeschaffung durch den Federal Reserve Act ins Leben gerufen wurde (Board of Govenors of the FED System, 1963; Federal Reserve Bank, 2015).

[31] Das Preisniveau ergibt sich aus dem Verhältnis zwischen dem realen Sozialprodukt und der Geldmenge. Unter Preisniveaustabilität wird dabei eine Beständigkeit von gleichbleibenden Preisen am Markt verstanden (Wildmann, 2007, S. 126-128).

notwendig erachtet, um im Falle von konjunkturellen Einbrüchen der Wirtschaft einem Abbau des Kapitalstocks[32] vorzubeugen, sowie übersteigerten Ansprüchen der Wirtschaft entgegenzuwirken. Dabei kann es in einer offenen Marktwirtschaft keine durchgehend starre Stabilität des Preises geben, da sich diese laufend entwickelt (Fand, 1970, S. 275-289; Cooper, 1974, S. 887-901). Aus diesem Grund wird im europäischen Raum von einem relativen Preissystem gesprochen. Wenn der Preis für Produkt A beispielsweise steigt, während der Preis für das ähnliche Produkt B gleichbleibt, so ist Produkt A im Verhältnis zu B relativ teurer geworden. Auf der anderen Seite ist Produkt B jedoch im Vergleich zu Produkt A relativ günstiger geworden. Diese Veränderungen in den Relationen werden am Markt von Verbrauchern und Herstellern registriert, welche darauf reagieren. Dies führt zu der Bezeichnung *relatives Preissystem* (Wildmann, 2007, S.126-129). Diese Bewegung in den Preisen der Güter lässt keine durchgehende Preisstabilität zu. Um Preisniveaustabilität zu messen, werden daher Kategorie-spezifische *Güterbündel* gebildet. Hierbei handelt es sich beispielsweise um durchschnittlich eingekaufte Waren für den Haushalt. Die Preise dieser Güter werden anschließend über einen bestimmten Zeitraum gemessen. Gleichen sich die Preisbewegungen aus, wodurch der Gesamtpreis der Güterbündel annähernd gleichbleibt, so liegt eine Preisniveaustabilität vor (ebd.). Eben diese versucht eine ZB überwiegend durch die Steuerung der Geldmenge zu erreichen. Ferner kontrollieren die Zentralbanken die Geldmenge zusätzlich über das Regulieren der Geschäftsbanken[33], bei welchen sie ihr Ziel über die Festsetzung von Zinsen und Mindestvorratsangaben erreichen können (Kapitel 2.3.3). Da eine ZB jedoch staatlich gebunden ist, vertritt diese auch politische Interessen, die über eine Stabilität der eigenen Währung hinausgehen können. Diese können zu einem weiteren Voranschreiten einer Inflation führen (ebd.).

2.3.4. Geldschöpfung durch Banken

Neben den Zentralbanken mit der Fähigkeit Geld[34] zu drucken, kommt es auch durch das Bankenwesen zu einer Vermehrung der Geldmenge. Geschäftsbanken nehmen im Gegensatz zu Zentralbanken im Kern die Rolle der Geldverwaltung der wirtschaftlichen Teilnehmer des Währungssystems – der Bürger, der Unternehmen und der Organisationen – ein (Wildmann, 2007, S. 115-121). Bei Banken bestehen dabei Unterschiede in der Ausprägung der Hauptgeschäftsfelder. Der Autor verzichtet hierbei bewusst auf

---

[32] Unter einem Kapitalstock wird das gesamte Sachkapital einer Volkswirtschaft verstanden. Beispiele hierfür sind etwa Maschinen, Gebäude, etc. (Kirchner, Poller & Morato Polzin, 2009).
[33] Bei Geschäftsbanken handelt es sich um Institutionen, die eine Bankenlizenz von der Zentralbank erhalten haben (ebd.)
[34] Es wird zwischen Geld, das durch die Zentralbank gedruckt wird (Zentralbankgeld) und durch Geldschöpfung von Geschäftsbanken entstandenes Geld (Buchgeld) unterschieden.

eine Analyse dieser, da der Bereich für das Verständnis und die Beantwortung der Forschungsfrage keine Relevanz aufweist. Die Funktion der Geldschöpfung lässt sich dagegen jedoch als sehr wichtig identifizieren, um einen Vergleich mit der Einheitenschöpfung Bitcoins ziehen zu können.

Geschäftsbanken schöpfen Geld mithilfe der *Kreditvergabe*. Banken erhalten hierbei Geld sowohl von der ZB zu gewissen Zinssätzen[35], sowie durch die Einlagen der Wirtschaftsteilnehmer. Gehen wir davon, dass Geschäftsbank A durch den Kunden Nummer 1 1000GE[36] erhält, so besitzt diese, wie in Abbildung 11 dargestellt, ein Geldangebot von 1000GE. Dabei müssen die Geschäftsbanken keine Mindestreserven an Geld für den Fall halten, dass der Kunde der Bank dieses ausgezahlt haben möchte. 2012 lag der Prozentsatz für die Mindestreserve bei 2%, aktuell ist dieser auf 0% gesetzt worden (Europäische Zentralbank, 2017).

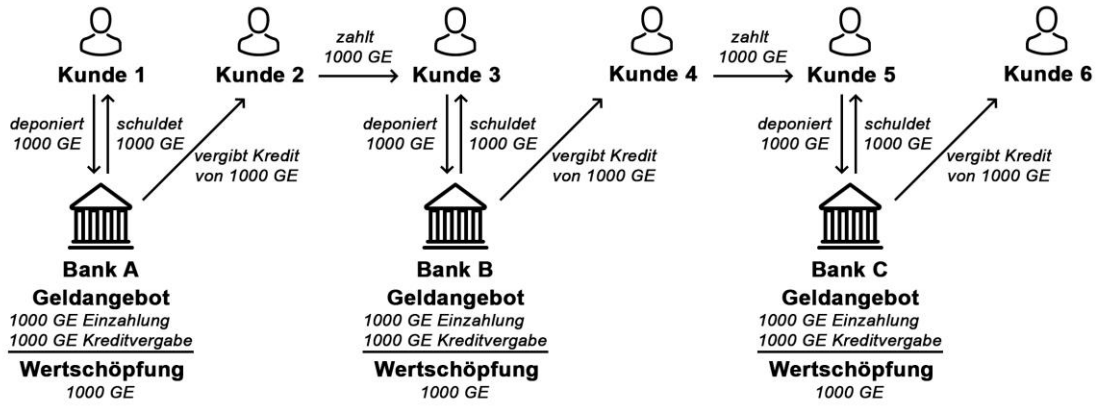

Abbildung 11: **Kreislauf der Geldschöpfung.** Quelle: Eigene Abbildung, 2018.[37]

Das bedeutet im Umkehrschluss, dass die Banken die gesamten 1000GE, die sie erhalten haben, weiterführend als Kredit vergeben können. Kunde 2 nimmt nun bei dieser Bank einen Kredit auf und begleicht damit eine Rechnung in Höhe von 1000GE bei Kunde 3. Da „der erste Kunde somit potenziell immer noch einen Anspruch auf die 1000GE geltend machen kann und der zweite Kunde faktisch auch 1000GE zur Verfügung hat, kann man argumentieren, dass das Geldangebot auf 2000GE gestiegen ist, bzw. 1000GE zusätzliches Geld geschöpft wurde." (Wildmann, 2007, S. 116-117). Kunde 3 zahlt wiederum das erhaltene Geld vollständig in seine Bank ein, welche den gleichen Prozess fortführen kann (siehe Abbildung 11). Die ursprünglichen, von der Zentralbank erhaltenen, 1000GE führen damit in der dargestellten Abbildung

[35] Banken übergeben im Gegenzug Wertpapiere. Dier Vorgang nennt sich Pansionieren (Europäische Zentralbank, 2009).
[36] In diesem Beispiel steht GE für Geldeinheiten. Dies dient der Vereinfachung und dem möglichen Bezug auf weitere Geldsysteme.
[37] In Anlehnung an Erläuterung von ebd.

nach drei Zyklen zu einer Geldschöpfung mit dem Multiplikator 3. 1000GE entwickeln sich hierbei zu 3000GE. Bei Mindestreserven von 0% kann dies zu einer Weitervergabe und Geldschöpfung bis ins Unendliche führen.

Die dargestellten Eigenschaften und Einflussfaktoren einer Währung verleihen dieser somit einen zentral gesteuerten inflationären Charakter. Die zentralen Herausgeber einer staatlichen Währung streben im Idealfall nach Stabilität dieser, verfolgen jedoch durch die Regierungsgebundenheit auch weitere nationale und internationale Interessen, die nicht zwingend auf eine solche Stabilität abzielen. Dies bringt Gefahren einer stärkeren Inflation mit sich, da der Gelddruck oft als internationalpolitisches Werkzeug genutzt wird (ebd.).

2.3.5. Gegenüberstellung zentraler Währungen und Bitcoin

Die vorigen Kapitel zeigen auf, dass eine zentrale Währung, ausgegeben durch den Staat oder einer von diesem vertrauten Instanz, die Eigenschaften des Strebens nach Wert- und Preisniveau Stabilität mit sich bringt, jedoch auch von anderen Einflüssen, wie internationaler Politik geleitet wird. Eine zentrale Währung erreicht im Idealfall ein Minimum an Volatilität und damit einhergehenden Preisschwankungen, birgt jedoch inflationäre Eigenschaften, die den Wert des Geldes auf Dauer nach unten treiben (Kessel & Alchian, 1962, S. 521–537). Dies wird durch die Steuerung der Banken erreicht, welche durch die genannten Möglichkeiten die Geldmenge einer Währung stetig erhöhen. Demgegenüber steht der Bitcoin als erste deflationäre Währung, dessen Preis sich einzig und allein durch den Markt bestimmt und durch die systemimmanente Endlichkeit der Einheiten diese deflationären Eigenschaften durch Verknappung maßgeblich unterstützt. Dabei hält sich das System des Bitcoin selbst aufrecht und bedarf keinem ausführenden und kontrollierenden Intermediär. Dies hat jedoch Asset-ähnliche Volatilität zur Folge, welche in Preisschwankungen und unvorhersehbaren Wertveränderungen resultiert.

2.3.6. Zentrale Zahlungssysteme

Da Währungen ein anderer Aufbau zugrunde liegt, sind diese im Gegensatz zu Bitcoin nicht Tausch-und Zahlungsmittel, sowie Zahlungssystem zugleich. Währungen können über verschiedene Bankensysteme transferiert werden. Hierbei erfordern verschiedene Anwendungszwecke die Nutzung verschiedener Zahlungssysteme. Aus diesem Grund ist es notwendig, einen Überblick über die Hauptaspekte von herkömmlichen Zahlungssystemen am Markt zu erarbeiten, um in einem anschließenden Vergleich mit Bitcoin dessen Chancen und Risiken hinsichtlich der Forschungsfrage zu ermitteln. Die

folgende Betrachtung beinhaltet dabei lediglich die Betrachtung der wesentlichen Aspekte hinsichtlich der Beantwortung der Forschungsfrage.

Bei diesen durchweg zentralen Zahlungssystemen gibt es Unmengen an Drittanbietern und große Unterschiede in den Ausprägungen. Zusammenfassend lässt sich jedoch sagen, dass es sich hierbei um zentrale Intermediäre handelt, bei denen der Kunde direkt oder über Drittanbieter über seine Bank bezahlt. Besitzt ein Kunde ein Konto bei einer Bank, so kann er auf verschiedenste Zahlungsmethoden zurückgreifen. Diese haben je nach Art der Bezahlung unterschiedlich hohe Transaktionsgebühren. Internationale Überweisungen beinhalten dabei die höchsten, nationale/unionsweite die geringsten. Als herkömmlichste Zahlungsmethode lässt sich dabei SEPA[38] identifizieren. Diese Methode stellt neben der immer weniger genutzten Standardüberweisung[39] eine EU-weite Zahlungsmethode dar. Die Transaktionsgebühren dieser variieren zwischen den jeweiligen Geschäftsbanken stark, liegen jedoch in den bekannten Fällen unter einem Euro (Comdirect, 2018). Eine solche Überweisung benötigt ein bis vier Werktage, bis sie ihren Empfänger erreicht hat, in der Regel jedoch nur einen. Außerhalb des EU-Raumes oder bei Überweisung in fremde Währungen kann die Auslandsüberweisung genutzt werden. Hierbei sind die Kosten jedoch „deutlich höher als für inländische oder SEPA-Transaktionen“ (Kauselmann, 2013). Auch bei Auslandsüberweisungen gilt die durchschnittliche Zeit von ein bis vier Werktagen. Beide Möglichkeiten lassen sich je nach Vereinbarung mit der jeweiligen Geschäftsbank online oder in den Filialen selbst tätigen. Mit Bankkonten verknüpfte *Electronic-Cash-Karten* (*EC-Karten*), ermöglichen dabei die bargeldlose Bezahlung am Point-of-Sale[40]. Der ausgegebene Betrag wird anschließend an eine Bezahlung mit dieser direkt vom Konto abgebucht. EC-Karten können nur innerhalb der nationalen Grenzen verwendet werden. Das letzte zu untersuchende Zahlungsmittel ist die Kreditkarte. Bei dieser wird das ausgegebene Geld oft erst gegen Ende des Monats kumuliert abgebucht, ein Einsatz im Ausland ist jedoch praktisch überall möglich.

---

[38] Bei der *Single Europe Payments Area* (SEPA) handelt es sich um eine Vereinfachung der EU-weiten Überweisungsabwicklung. Dabei werden Überweisungen nur in der Währung Euro abgewickelt und weisen sowohl national, als auch international innerhalb des SEPA-Raumes die gleichen Kosten auf. Ziel SEPAs ist es, den europäischen Raum bargeldlos zu gestalten (Deutsche Bundesbank, 2018).

[39] Die national nutzbare Standardüberweisung wird individuell von den jeweiligen Geschäftsbanken ausgeführt und nutzt im Gegensatz zu SEPA kein einheitliches System, weswegen hierbei höhere Kosten anfallen.

[40] Beim Point of Sale handelt es sich um die jeweilige Verkaufs- oder Einkaufsstelle an denen Waren angeboten werden. Hierbei kann es sich sowohl um physische Betriebe, als auch um Onlinehändler handeln (Schneider, 2018).

2.4. Zusammenfassung der theoretischen Erkenntnisse

Die Auseinandersetzung mit der Funktionsweise Bitcoins und der Blockchain zeigt auf, dass diese und deren Teilnehmer des Ökosystems ein dezentrales, intermediärloses und fälschungssicheres Tausch- und Zahlungsmittel ermöglichen, welches seinen Wert durch den Markt selbst bestimmt und ein transparentes und demokratisch konsensfindendes Netzwerk darstellt. Bitcoin bietet als Tausch-und Zahlungsmittel einen alternativen Ansatz zu herkömmlichen Währungen, ist jedoch als Zahlungsmittel sowohl durch die deflationären Eigenschaften, als auch die systemimmanenten Skalierungsprobleme nicht konkurrenzfähig. Dies ist vor allem auf die Volatilität des Assets zurückzuführen, welche dadurch weitaus mehr Risiken bei der Nutzung als Zahlungsmittel birgt, als eine zentral gesteuerte souveräne Währung. Auch die systemimmanenten Skalierungsprobleme lassen sich ohne die Nutzung von Drittanbietern wie dem Lightning Network langfristig nicht beheben und haben hohe Transaktionskosten und -zeiten zur Folge, welche eine Nutzung als Tausch-und Zahlungsmittel unwirtschaftlich gestalten. Währungen durchlaufen den Prozess der zentralen Geldschöpfung, welche durch die Intermediäre Zentralbanken und Geschäftsbanken durchgeführt und kontrolliert werden. Diese erreichen durch den Eingriff in das System die Preisstabilität, die Bitcoin auch in naher Zukunft nicht bieten kann. Die zentralen Zahlungsmethoden bieten darüber hinaus eine andere Art der Flexibilität. Der Nutzer kann sich bei diesen zwischen diversen Optionen entscheiden und beispielsweise durch Kreditkarten erst am Ende eines Monats bezahlen. Diese Möglichkeiten können jedoch theoretisch auch über Drittanbieter am Markt für Bitcoin umgesetzt werden. Dies ist aktuell jedoch nicht der Fall.

Aus diesen Gründen stellt Bitcoin zwar einen dezentralen Ansatz gegenüber den zentralen Mitteln dar, erreicht jedoch durch die aufgezeigten Risiken und das Fehlen von maßgeblichen Vorteilen gegenüber stabilen, souveränen Währungen, nur Chancen in dessen Nutzung als Alternative. Mögliche Gründe für die Nutzung einer solchen sind beispielsweise die Unzufriedenheit mit der jeweiligen staatlichen Handhabung der eigenen Währung. Die Nutzung eines anderen Zahlungsmittels war bisher innerhalb der Ländergrenzen nicht möglich. Dennoch ist die Nachfrage einer Nutzung dieser alternativen Möglichkeit aktuell durch die geringe Akzeptanz der Händler am Markt als geringfügig einzustufen. Bezüglich der gesetzlichen Einflüsse auf die Nutzung Bitcoins als Tausch-und Zahlungsmittel bot jegliche untersuchte Literatur aufgrund der Neuheit des Themas keine fundierten Fakten. Aus diesem Grund wird die Frage nach diesen in den Fragebogen verlegt und bedarf erst in der qualitativen Inhaltsanalyse einer tiefgreifenden Betrachtung.

3. Analyse der Chancen und Risiken

Anschließend an die in den vorigen Kapiteln erfolgte Erarbeitung der Grundlagen Bitcoins, sowie der Theorie der zu vergleichenden Währungen, widmet sich der folgende Teil dieser Arbeit der qualitativen Analyse der *Chancen und Risiken von Bitcoin als Tausch-und Zahlungsmittel*. Im Hinblick auf die Durchführung der qualitativen Inhaltsanalyse werden anfangs (Hypo-)[41] These(n) formuliert, welche der empirischen Untersuchung zugrunde liegen. Diese gilt es mit Hilfe der ausgewählten Forschungsmethode zu verifizieren und/oder zu falsifizieren. Des Weiteren werden sechs relevante Kategorien definiert, die der Darstellung der Forschungsergebnisse dienen. Der abschließende Teil widmet sich der fundierten Beantwortung der Forschungsfrage, unter anderem mittels der Überprüfung der Annahmen. Die Forschungsfrage: „*Welche Chancen und Risiken ergeben sich in der Nutzung von Bitcoin als Tausch-und Zahlungsmittel?*“ berücksichtigend, stellt der Autor die folgende These auf: *Bitcoin bieten sich im aktuellen technischen Zustand geringe Chancen als Tausch- und Zahlungsmittel in der breiten Menge genutzt zu werden*. Zwecks Spezifizierung dieser These gilt es nun, Hypothesen von dieser abzuleiten: (1) *Die hohen Transaktionszeiten verhindern eine effiziente Nutzung von Bitcoin als Zahlungsmittel*. (2) *Die hohen Transaktionskosten machen eine ökonomisch effiziente Zahlung nicht möglich*. (3) *Die hohe Volatilität des Assets hat hohe Preisschwankungen zur Folge, welche Risiken, sowohl auf der Käufer-, als auch auf der Verkäuferseite erzeugen*. (4) *Die technischen Nachteile gegenüber herkömmlichen Zahlungsmitteln sind als systemimmanent zu betrachten und können nicht ohne die Inanspruchnahme von zentralen Drittanbieter-Services umgangen werden*.

3.1. Auswahl der Forschungsmethoden

Um eine wissenschaftliche Beantwortung der Forschungsfrage zu gewährleisten, wurden im Dezember 2017 insgesamt acht Experten aus verschiedenen Bereichen, welche alle starke Berührungspunkte mit dem Themengebiet aufweisen, befragt. Dabei wurde bei der Auswahl auch auf die Erreichung eines vielseitigen Expertenpools geachtet, welcher zu einer möglichst objektiven und fundierten Betrachtung aus verschiedenen Perspektiven beitragen konnte. Eine Auswertung der Interviewtexte erfolgte im Anschluss systematisch. Die folgenden beiden Abschnitte dienen sowohl der Begründung der Auswahl der gewählten Forschungsmethode hinsichtlich der zu

[41] „Unter einer Hypothese versteht man in der empirischen Sozialforschung eine anhand empirischer Daten zu prüfende Annahme. Im Rahmen der quantitativen (standardisierten) Sozialforschung meint man vor allem eine Annahme, die einem statistischen Test unterworfen werden kann. Diese Annahme richtet sich meistens darauf, dass zwischen zwei Merkmalen ein Zusammenhang, oder dass zwischen Gruppen ein Unterschied besteht. […]“ (Kromney, 2007, S. 341).

beantwortenden wissenschaftlichen Fragestellung, als auch der Erläuterung wichtiger Einzelheiten. Bei Letzterem handelt es sich um die Darstellung der gewählten analytischen Vorgehensweise, eine Vorstellung der befragten Experten[42] und des angewandten Interviewleitfadens[43], sowie eine Bildung entscheidender Kategorien als Werkzeug der Inhaltsanalyse.

3.1.1. Das leitfadengestützte Experteninterview

Die Erarbeitung der theoretischen Erkenntnisse hinsichtlich der Chancen und Risiken Bitcoins als Tausch- und Zahlungsmittel zeigte auf, dass sich das Krypto-Asset im derzeitigen technischen Zustand und im Vergleich zur zentralen Alternative wenig als Handelsmedium eignet, was auf verschiedene systemimmanente und marktwirtschaftliche Faktoren zurückzuführen ist. Weitere Einflussfaktoren, wie die des Rechtsraumes oder der Einschätzung der Stabilität des Ökosystems konnten jedoch im Rahmen der theoretischen Erkenntnisse nicht ausreichend bestimmt werden. Dieser Grund macht es notwendig, die erarbeiteten Erkenntnisse mit weiterem Fachwissen anzureichern und zu bestätigen. Im Gegensatz zu quantitativen Forschungsmethoden, deren vorrangiges Ziel es ist, zahlenmäßige Sachverhalte abzubilden, verfolgen qualitative Methoden dabei das Ziel, kleine Stichproben mittels einer empirischen Analyse zu erkunden, um hierbei neues, relevantes Wissen zu erschließen und gegebenenfalls Maßnahmen für mögliche weitere Forschungen abzuleiten (Brosius, Koschel & Haas, 2009, S. 19-21). In dieser Arbeit wird die *Wissensaneignung* der qualitativen Forschung genutzt, in welcher das bisherige Wissen weiterführend mit Spezialwissen zu ergänzen ist, um eine Detailierung der abschließenden Interpretation im Hinblick auf die Forschungsargumentation erreichen zu können (Gläser & Laudel, 2010, S.111). Die in dieser Arbeit genutzte Methode der Datenerhebung stellt daher das *leitfadengestützte Experteninterview* dar. Bei diesem werden Experten einer Disziplin zu Rate gezogen, um eben dieses Spezialwissen zu erhalten, welches der Forschende nicht ohne dessen Hilfe zu erlangen vermag. Der Terminus *leitfadengestützt* kann dabei synonymhaft für den Begriff *teilstandardisiert* verstanden werden, da die Leitfragen des Interviews, abgeleitet aus den Hypothesen, das Grundgerüst für dieses darstellen, die Abfolge dieser Fragestellungen jedoch variieren kann (ebd.). Auch kann auf Nachfragen eingegangen werden. Durch eine Übersetzung der Leitfragen in Interviewfragen können diese „an den Alltag des Interviewpartners anschließen." (ebd.,

[42] Experten sind Personen, die „auf dem Gebiet, das es zu untersuchen und zu explizieren gilt, einen [...] Wissensvorsprung gegenüber dem Forschenden haben. Sie sind die Sachverständigen und können als Gutachter agieren, aufklären und einschätzen z.B. Risiken und Gefahren von Technologien, damit verbundene Veränderungen von Rezeptions- und Aneignungsweisen [...]." (Hoffmann, 2005, S.314).
[43] (Anhang 1)

S. 142). Im Zuge dieser empirischen Untersuchung wurden insgesamt zehn Leitfragen und etwaige Nachfragen für die Interviews entwickelt. Dabei fand eine inhaltliche Vorbereitung vor jeder dieser statt, um Aufnahmebereitschaft, großes Interesse am Thema und Wissen zu signalisieren, mit dem Ziel die schöpfbare Menge des Spezialwissens zu maximieren (ebd., S. 148). Die Interviews wurden elektronisch aufgezeichnet und für die qualitative Inhaltsanalyse vollständig transkribiert (ebd., S. 193).

3.1.2. Die Experten

Bei der Auswahl der Experten wurde wie eingangs berichtet, stark darauf geachtet, dass bei einem komplexen Thema wie dem vorliegenden, eine fundierte und umgreifende Betrachtung der Forschungsfrage garantiert werden kann und annähernde Repräsentativität der Forschung, trotz der geringen Fallzahl von acht Experten, durch eben diese Erreichung eines umfassenden Gesamtbildes erzeugt wird. Hierbei ergaben sich drei relevante Berufsfelder, aus denen Experten den größten Mehrwert hinsichtlich der Beantwortung der Forschungsfrage dieser Arbeit bieten konnten: Finanz- und Bankenwesen, Softwareentwicklung mit Blockchainbezug und Rechtswesen. Der folgende Abschnitt stellt dementsprechend die Experten und ihre Berührungspunkte mit dem Thema vor[44].

Der erste Experte, Christopher Nigischer, ist Managing Partner der *Chainstep GmbH*, welche Unternehmen durch Beratung, Schulungen und Applikationsentwicklungen im Rahmen der Blockchaintechnologie unterstützt. Hierzu gehört auch ein Fokus auf der ICO-Beratung[45] und -umsetzung für jeweilige Anwendungsfälle. Zusätzlich kümmert sich Nigischer als Initiator des *Innovationsforums Blockchain* um die Finanzierung des Forums, welches, vom Bundesministerium für Bildung gefördert, Konferenzen und Meetups für mittelständische Unternehmen organisiert. Ziel ist ein Austausch und eine Vernetzung untereinander. Weiterführend arbeitet Nigischer als Projektmanager für Cooperative Innovation Projects in der *NXP Semiconductors Germany*, einem global führenden Unternehmen im Bereich Datenverarbeitung, Datenverbindung und Sicherheit mit Firmensitzen in 33 Ländern, an der Identifikation von innovativen Tech-

[44] An dieser Stelle sei darauf hingewiesen, dass Experten in Unternehmen, die mit der Blockchaintechnologie arbeiten, zwar indirekt durch eine Aufmerksamkeit des Bitcoin profitieren können, jedoch keine ersichtlichen Vorteile bei einer Agenda-beeinflussten, positiv verfälschten Wahl der Antworten hinsichtlich der Beantwortung der Forschungsfrage, erhalten.

[45] Bei ICOs (Initial Coin Offerings) handelt es sich um die Einbindung eines Tokens in das Netzwerk des Unternehmens im Hinblick auf den jeweiligen Use-Case. Dies wird unter anderem mit dem Ziel durchgeführt, Kapital für das Unternehmen zu erwirtschaften, indem dieser Token verkauft und an Wert gewinnen wird. Beispiel hierfür ist die Firma Kodak, welche mit ihrem Token die Bildrechte der Künstler fälschungssicher auf der Ethereum-Blockchain zu speichern versucht (Drescher, 2017; Kodak, 2018).

nologien, sowie der Umsetzung von Projekten mit diesen. Im Zuge dessen ist Nigischer mit der Architektur Bitcoins und dessen Ökosystem bestens vertraut.

Als zweiter Experte wurde Daniel Heller interviewt. Heller befasst sich aktuell am *Petersen Institute for International Economics* (PIIE) mit der kritischen Untersuchung digitaler Währungen und damit einhergehend auch mit Bitcoin. Durch seinen umfassenden Hintergrund als Generalsekretär des *Commity on Payments and Settlement System*[46], einem Komitee internationaler Zentralbanken, sowie vorheriger leitender Funktionen in der Schweizer Nationalbank, in welchen er sich mit Themen von Systemrisiken, über Retail-Payments bis hin zu Finanzstabilität beschäftigte bringt Heller damit einen großen Wissensschatz mit, der der Beantwortung der Forschungsfrage von großem Nutzen ist.

Florian Fiedler, Geschäftsführer des Unternehmens *Blockbay*, ist der dritte Experte. Aus der Strategieberatung kommend, führte Fiedler diverse Projekte auf Vorstandsebene für Banken im In-und Ausland durch, darunter Gründung, Verkauf und Merger zwischen Banken, und arbeitete anschließend im gleichen Bereich für *IBM* Deutschland, Österreich und Schweiz. In der darauffolgenden Stelle als Chief Technical Officer (CTO) der *HSH-Nordbank*, ergaben sich für Fiedler erste Berührungspunkte mit Bitcoin und der Blockchaintechnologie, wobei Letztere unter seiner Leitung als Projekt zu Testzwecken implementiert wurde. Die Potenziale dieser erkennend, gründete Fiedler anschließend sein aktuelles Unternehmen *Blockbay*, welches an einer Vereinfachung des effizienten Kryptohandels am Markt strebt.

Daniel Jeffries wurde als Autor und Unternehmer in Los Angeles im Bereich der Blockchaintechnologie als vierter Experte ausgewählt. Jeffries verfasst Artikel rund um das Thema Blockchain und Kryptowährungen in global gelesenen, themenbezogenen Technologiemagazinen, wie *Medium* und *BitcoinMagazine*. Durch seine über zwei Jahrzehnte umfassende IT-Erfahrungen greift er bei der Analyse von aufkommenden Kryptowährungen auf dieses Wissen zurück. Als Fachautor befasst er sich dabei täglich mit den Veränderungen am Markt und korrespondiert mit diversen Experten. Besonders fokussiert er sich auf mögliche zukünftige Szenarien, deren negativen Aspekten er durch Lösungsvorschläge in seinen Artikeln vorzubeugen versucht.

[46] Das Komitee der Schweizer Bank für internationalen Zahlungsausgleich (BIZ), setzt sich aus Mitgliedern 60 verschiedener, internationaler Zentralbanken zusammen, und befasst sich mit der internationalen Währungs- und Finanzstabilität, sowie der Finanzmarktlage und fördert die Zusammenarbeit der Teilnehmer international (BIZ, 2017). Neben weiteren Markt- und Bankenaufsichtsangelegenheiten verwahrt die BIZ auch Teile der Geldreserven für Aktionäre wie die Federal Reserve Bank, die Europäische Zentralbank, sowie Teile der internationalen Währungsreserven (ebd.).

Überdies arbeitet Jeffries selbst als Entwickler an einem Blockchainprojekt, welches unter anderem starken Bezug zu Bitcoin aufweist. Die genauen Informationen zu diesem Projekt möchte er in der vorliegenden Arbeit nicht preisgeben.

Die fünfte Expertin ist Darshini Dalal. Sie ist Leiterin des Blockchain Labs in der *Deloitte Consulting LLP* in Boston und befasst sich als *Technology Strategist* täglich mit den Möglichkeiten und Risiken der Technologie. Dalal berät Klienten weltweit und klärt diese über die möglichen Anwendungsmöglichkeiten dieser auf. Des Weiteren begleitet sie dabei den Prozess von der Erstellung der Vision bis hin zur wirtschaftlichen Umsetzung dieser, wie zum Beispiel der Implementierung eines funktionsfähigen Blockchainsystems. Zusätzlich berät Dalal ehrenamtlich die Zentralbank Singapurs, die *Monetary Authority of Singapur* in finanzstrategischen Aspekten.

Als sechster Experte wurde Prof. Dr. Bernd Thomas Ramb, Diplommathematiker und promovierter sowie habilitierter Volkswirt, ausgewählt. Der Emerit legt seine Forschungsschwerpunkte auf die allgemeine Wirtschaftspolitik, die Geldtheorie und Geldpolitik und weiterführend die ökonomische Verhaltenstheorie. Im Zuge einer Analyse der Fallstricke der Eurowährung ergaben sich Rambs erste Berührungspunkte mit dem Thema Bitcoin direkt nach dessen Aufkommen vor ungefähr acht Jahren, nach welcher er sich umfassend mit diesem beschäftigte. Ramb bringt damit einen hochwertigen theoretischen Hintergrund mit sich, welcher die Leitfrage von einer weiteren Perspektive betrachten kann.

Benjamin Kirschbaum ist als Rechtsanwalt der Kanzlei *Winheller Rechtsanwaltsgesellschaft mbh* der siebte Experte im Bunde. Aufgrund von beruflichen und privaten Berührungspunkten mit Kryptowährungen konzentriert sich Kirschbaums Fokus aktuell auf Rechtsfragen zu dem Thema Blockchain und Kryptoassets/-währungen. Hierbei berät der Experte vor allem finanztechnische Unternehmen hinsichtlich eines rechtssicheren Aufbaus der Unternehmensstrukturen. Neben steueroptimierenden Gestaltungen steht dabei die Zusammenarbeit mit der Bundesanstalt für Finanzdienstleistung (BaFin) im Vordergrund. Kirschbaum ist als Experte in der Lage, die Fragestellung hinsichtlich der rechtlichen Einflüsse auf eine Nutzung Bitcoins als Zahlungsmittel, sowie deren Auswirkungen, ausführlich zu beantworten.

Der achte und letzte Experte ist Patrick Charrier. Als Softwareentwickler der Firma *Blockchain Helix* liegt sein Hauptaufgabenbereich auf dem Programmieren von Smart-

contracts für die Blockchain *Ethereums*, mit dem Ziel, Identitätsmanagement auf der Blockchain aufzubauen. Zusätzlich arbeitet Charrier auch an Projekten weiterer Unternehmen, unter anderen an einem möglichen ICO für ein Rewardsystem der Firma *Crytek*. Nebenbei arbeitet Charrier außerdem an dem Aufbau einer Mining-Farm in Tschechien.

3.2. Qualitative Inhaltsanalyse

Als Methode zur Analyse der erhobenen Daten wird in dieser Arbeit die qualitative Inhaltsanalyse eingesetzt. Diese will laut Mayring (2002), Professor für psychologische Methodenforschung und mitwirkender Entwickler dieser, „[...] Texte systematisch analysieren, indem sie das Material schrittweise und theoriegeleitet am Material entwickelten Kategoriensystemen bearbeitet." (Mayring 2002, S. 114). Spezifiziert erfordert die in diesem Fall angewandte „Kategorie-geleitete Textanalyse" (ebd., S. 13) in diesem Fall Systematik in dem Analysevorgehen mit dem Ziel, die relevanten Informationen hinsichtlich der Beantwortung der Forschungsfrage zu extrahieren und zu aggregieren (ebd.). Bei dem Kategoriensystem handelt es sich um aus dem theoretischen Teil und den Hypothesen abgeleitete Analyseregeln, anhand derer die Auswertung maßgeblich erfolgt. Die Experteninterviews werden hierbei deduktiv, anhand vorab in einem Kategoriensystem (Codebuch) festgelegter Regeln, strukturiert. Hierbei orientiert sich dieses an den Interviewfragen, welche basierend auf der Forschungsfrage und den (Hypo-) These(n) entwickelt worden sind (siehe Tabelle 1).

	Kategorie	**Interviewfrage(n)**
1	Definitorische Einstufung	Als welche Art von Medium ist Bitcoin zu definieren?
2	Technische Effizienz	Als wie effizient ist die System-Architektur der Blockchain zu betrachten? Welche Chancen und Risiken lassen sich in dieser im Hinblick auf eine Nutzung als Tausch-und Zahlungsmittel identifizieren?
3	Ökonomische Effizienz	Kann die Nutzung Bitcoins ökonomisch effizient gestaltet werden? Welche Probleme ergeben sich durch die Volatilität des Bitcoins?
4	Technische Sicherheit und Usability	Als wie sicher ist die Nutzung der Blockchain zu erachten? Wie einfach gestaltet sich die Durchführung einer Transaktion? Entstehen Risiken durch die Zentralisierung der Miningpools?
5	Gesetzliche Einflüsse	Welche finanz- und steuerrechtlichen Rahmenbedingungen herrschen bei der Nutzung von Bitcoins als Tausch- und Zahlungsmittel für private/juristische Personen?

6	Stabilität des Ökosystems	Gibt es fragile Knoten im Blockchan-Netzwerk? Welche Risiken und/oder Chancen ergeben sich durch den elitären Kreis der Entwickler und Nodebetreiber?

Tabelle 1: **Deduktives Kategoriensystem der qualitativen Inhaltsanalyse - Inhaltliche Strukturierung.** Quelle: Eigene Darstellung, 2018.

Um eine wissenschaftlich korrekte Extraktion der zu der jeweiligen Textstelle passenden Kategorie zu gewährleisten, gilt es das Verhalten vorab mit folgender Kodierregel abzusichern: Wurde auf eine oder mehrere Fragen der jeweiligen Kategorie themenbezogen geantwortet, so ist diese Textstelle der vorliegenden Kategorie zuzuordnen. Des Weiteren wird die Strukturierung dieser deduktiven Kategorienbildung für ein systematisches Vorgehen hinsichtlich des Inhalts vorgenommen. Diese Methode der *Inhaltlichen Strukturierung* „will Material zu bestimmten Themen, zu bestimmten Inhaltsbereichen extrahieren und zusammenfassen." (Mayring, 2002, S.99). Relevante Textpassagen werden demnach durch eine farbliche Kennzeichnung einer der sechs gebildeten Kategorien zugewiesen und können anschließend in einer Excel-Datei strukturiert geordnet werden. Diese Übersicht[47] bildet die Kernaussagen der Experten zu den jeweiligen Kategorien ab und überprüft diese auf Übereinstimmung hinsichtlich der abgeleiteten (Hypo-) These(n). Informationen, die aus diesem Prozess hervorgehen, sind dementsprechend qualitativer Natur. Abschließend sei darauf hingewiesen, dass über den gesamten Forschungsprozess hinweg stets auf die Einhaltung der Gütekriterien Systematik (methodisches Vorgehen), Objektivität (Nachvollziehbarkeit des methodischen Vorgehens), Reliabilität (Verlässlichkeit der Forschungsmethode) und Validität (Gültigkeit) geachtet wurde (Kaiser, 2014, S.39).

3.3. Analyseergebnisse

Das folgende Kapitel befasst sich mit der Darstellung der analysierten Ergebnisse, welche im Zuge der qualitativen Inhaltsanalyse anhand der sechs definierten Kategorien extrahiert und analysiert wurden: „Definitorische Einstufung Bitcoins", „Technische Effizienz", „Ökonomische Effizienz", „Systemsicherheit und Usability", „Stabilität des Ökosystems" und „Gesetzliche Einflussfaktoren.

3.3.1. Definitorische Einstufung Bitcoins

Eine Währung definiert sich durch die inhärenten Eigenschaften der Nutzung als in einem staatlichen Wirtschaftssystem überwiegend akzeptiertes Tausch-und Zahlungsmittel, die Nutzbarkeit als Recheneinheit, sowie der Funktion als

[47] Siehe Anhang 2: Übereinstimmung: grün; Ähnlichkeit (grau); Unterschied (rot)

Wertspeicher (Wildmann, 2007, S. 106-109). Sind alle Eigenschaften erfüllt, gilt das untersuchte Objekt als Währung.

Übereinstimmung hinsichtlich der unzutreffenden Definition Bitcoins als Währung ist bei Heller vom Petersen Institute for International Economics und Fiedler, Geschäftsführer von Blockbay zu finden. Heller (2017), ehemaliger Generalsekretär des Schweizer *Commity on Payments and Settlement Systems*, sieht die technische Funktion von Bitcoin als Tausch- und Zahlungsmittel als erfüllt an (Z. 33-36). Die Eigenschaft, als Recheneinheit genutzt werden zu können, spricht Heller dem hybriden Asset ab: „Die Fluktuation ist viel zu hoch um als Recheneinheit geeignet zu sein." (ebd.). Auch kann es nicht als Wertspeicher genutzt werden, da Unklarheit besteht, ob und wie lange sich das Vertrauen in das System hält (ebd.). Fiedler (2017), ehemaliges Mitglied im Vorstand der HSH-Nordbank, begreift auch die Funktion als Tausch- und Zahlungsmittel als „eingeschränkt" (Z. 264). Technisch ist es als solches nutzbar, angesichts der hohen Transaktionskosten[48] jedoch für Zahlungen einer geringen Höhe unbrauchbar (Z. 249 ff). Fiedler (2017) weist darauf hin, dass eine Währung in einem Wirtschaftssystem von der überwiegenden Anzahl der Zahlungsempfänger akzeptiert werden muss, wobei Bitcoin als „absolut nicht massenkompatibel" (Z. 257-258) einzustufen ist (ebd.). Im Gegensatz zu Heller spricht Fiedler Bitcoin den Aspekt der Nutzung als Recheneinheit nicht gänzlich ab, sondern ordnet diesen auch als begrenzt ein. Fiedler (2017) verweist dabei auf die Paarung der über 1300 Krypto-Assets mit Bitcoin an den Krypto-Börsen, an denen Bitcoin als funktionierende Recheneinheit genutzt wird, um zu prüfen, in welcher Höhe Gewinne oder Verluste im Vergleich zum Bitcoin realisiert wurden (Z. 261-270). Gleichgesetzt werden kann dieser Vorgang mit dem Kauf einer Aktie an der Börse und dem Vergleichen mit dem DAX[49], oder mit einer einzelnen Aktie (ebd.). Fiedler (2017) sieht die hohe Volatilität jedoch auch als ein Kriterium gegen die vollends erfüllte Definition als Recheneinheit (ebd.). Fiedler (2017) verweist weiterhin zum Thema Wertspeicherung auf Länder wie Venezuela, in denen das Volk der Landeswährung misstraut und den Bitcoin, trotz der Volatilität als Wertspeicher nutzen kann: „Das ist auch ein Nachteil von den Zentralbanken, es bestehen ja nicht nur Vorteile, die können ja nach Belieben Geld nachdrucken. Dadurch entsteht dann oft eine riesen Inflation und wenn die Leute [...] ein Gehalt von 1000 Dollar bekommen, und im nächsten Monat ist das nur noch 800 wert, oder noch weniger. Und um sich davor zu schützen, in diesen Ländern, ist dies ein wunderbares

[48] Die Höhe der Transaktionskosten lag zum Zeitpunkt des Interviews bei 12$ und stieg im Januar (Stand 10.01.2018) auf 29$ pro Transaktion an (BitInfoCharts, 2018).
[49] Der Deutsche Aktien Index (DAX) enthält Aktien der 30 wirtschaftlich stärksten und liquidesten Unternehmen am deutschen Aktienmarkt. Vergleicht sich ein Aktionär, der nicht in diesen investiert hat, mit dem DAX, so überprüft er, ob sein eingesetztes Kapital, im Vergleich zum DAX, prozentual besser oder schlechter performt hat (Deutsche Börse, 2016).

Wertspeicherungssystem. [..] Ja, ich habe die Volatilität des Bitcoins, aber im Vergleich zu dem Risiko, dass meine Regierung mit meinem Geld Schabernack treibt, nehmen viele die Volatilität in Kauf und sehen darin viele Vorteile.“ (Z. 278-298). Im Europäischen Raum und vor allem in Deutschland sieht Fiedler (2017) die Funktion als Wertspeicher, bei welchem der Wert auf lange Zeit abzusehen ist, jedoch nicht als erfüllt an (Z. 278-287). Der Bitcoin hat gewisse währungsähnliche Eigenschaften, ist jedoch nicht als eindeutig als solche per Definition zu verstehen (ebd.).

Ähnlichkeiten hinsichtlich der Frage nach der Definition finden sich auch bei Ramb, emeritierter Diplommathematiker und Volkswirt mit Forschungsschwerpunkten auf Wirtschaftspolitik, Geldtheorie und Geldpolitk. Ramb (2017) begreift Bitcoin nicht als Währung und weist weiterhin daraufhin, dass auch viele klassische, nationale Währungen wie der Euro qua Definition nicht mehr die Kriterien einer Währung erfüllen, überwiegend aus dem deflationären Grund, dass diese den Wert auf lange Zeit nicht mehr speichern, sondern verringern (Z. 207-217). Laut Ramb ist der Bitcoin definitorisch nicht als Währung einzustufen, am Markt jedoch mit zunehmender Attraktivität und Abnahme der Volatilität immer mehr als solche zu behandeln (2017, ebd.).

3.3.2. Technische Effizienz

Übereinstimmung hinsichtlich der Aspekte der technischen Effizienz Bitcoins in der Nutzung als Zahlungsmittel lässt sich kollektiv in den Aussagen aller Experten identifizieren. Charrier (2017), Blockchainentwickler mit dem Schwerpunkt auf Smart-Contracts, sieht in dem dezentralen Peer-to-Peer System Bitcoin ein Netzwerk mit großem technischen Potenzial (Z. 259-271). Die aktuell langen Transaktionszeiten sind jedoch ein Produkt des Skalierungsproblems, welches sich technisch ohne Drittanbieter mit einer Off-Chain Lösung nicht vollends beheben lässt (ebd.). Charrier (2017) bezieht sich dabei auf das, in Kapitel 2.2.4.3 vorgestellte, Lightning-Network, durch welches die Transaktionen Off-Chain durch einen zentralisierten Drittanbieter realisiert und anschließend gebündelt an die Blockchain kommuniziert werden. Dadurch entstehen sowohl geringe Transaktionskosten im Centbereich, als auch Transaktionszeiten um die zwei Sekunden, welche eine komplett neue Effizienz in der Nutzung von Bitcoin erreichen, ganz im Gegensatz zu den hohen Transaktionskosten und -zeiten von durchschnittlich 25$ und 268 Minuten[50] auf der Blockchain an sich. Des Weiteren können auch Protokolle wie das *NextGenerations-Protocoll*, bei welchem

[50] Die Durchschnittswerte wurden der Plattform Blockchain.info entnommen und bilden die durchschnittliche Transaktionszeit und Transaktionskosten der Blockchain in der Woche der Enthebung ab (2018).

die Blöcke nicht alle 10 Minuten akzeptiert werden, sondern Miner vorausschauend winzige Blöcke mit jeweils einer Transaktion kreieren, die dann von einem, alle 10 Minuten zufällig auserwählten Miner, zu einem großen Block zusammengefügt werden, wie beim Lightning-Netzwerk, nur durch einen anderen Ansatz, die Transaktionszeiten und -kosten maßgeblich gesenkt werden können (ebd.). Laut Charrier liegt die Kernkompetenz von Bitcoin daher überwiegend in der Sicherheit des Systems, welches seit Entstehung nicht gehackt werden konnte, da ein Angriff sich auch durch die erforderlichen Ressourcen nicht als wirtschaftlich erweisen würde (2017, Z. 233-255).

Heller (2017) weist wie Charrier auch darauf hin, dass die Massentauglichkeit von Bitcoin On-Chain durch das Kapazitätslimit nicht gegeben ist und eine Off-Chain Lösung, wie das Lightning-Network, eine zentrale Alternative darstellt, um Bitcoin als Zahlungsmittel sinnvoll verwenden zu können (et al.). Des Weiteren zieht er einen Vergleich zu den konventionellen Zahlungsmitteln, die „unglaublich schnell“ (Z. 68-70) geworden sind und Retail-Payments in zwei Sekunden abwickeln können (ebd.). Heller (2017 stellt sich die Frage, ob „Bitcoin überhaupt Konkurrenz zu herkömmlichen Zahlungsmethoden darstellen kann?“ (Z. 72-74). Eine Konkurrenzfähigkeit Bitcoins wäre nur durch Drittanbieter möglich, die jedoch keine Vorteile, sondern nur eine Alternative zu den bereits im Wirtschaftssystem vollintegrierten Systemen bieten (ebd.). Einen weiteren Nachteil sieht Heller (2017) als ehemaliger Generalsekretär des Schweizer „Commity on Payments and Settlement System“ (Z. 8-13), in der Dauer bis zur Unumkehrbarkeit der Zahlungen, die bei Bitcoin ungefähr eine Stunde beträgt, bis eine Zahlung vollends bestätigt und von jeder Node verzeichnet wurde (133-136). Sollte eine Bank 100 Millionen Euro überweisen, so „will sie eine sofortige Bestätigung und nicht eine Stunde warten.“ (Z. 133-137). Auch in der Nutzung als Handelsmedium im Alltag der Bürger kann Heller (2017) keinen technischen Vorteil identifizieren und klassifiziert Bitcoin daher lediglich als eine mögliche Alternative mit keinen wesentlichen Vorteilen, bei welcher eine Integration am Markt noch erforderlich ist (Z. 81-85).

Hinsichtlich der untersuchten Kategorie sind auch Fiedlers Aussagen ähnlich einzustufen. Fiedler (2017) setzt dabei als Ex-Vorstandsmitglied der HSH-Nordbank das Bitcoinnetzwerk in Relation mit dem Visa-Netzwerk (Z. 124-129). Das Bitcoinnetzwerk wird ohne die Nutzung von Drittanbietern „niemals so weit verbessert werden, dass Transaktionen im Massenvolumen, vergleichbar zum Beispiel mit VISA [...] ermöglicht werden.“ (Z. 126-131; Kapitel 2.3.5). Konkurrenz sieht Fiedler dabei nicht nur in herkömmlichen Zahlungsmethoden, sondern auch in virtuellen Währungen, die aufgrund ihrer Eigenschaften definitorisch, im Gegensatz zu Bitcoin auch als solche

zu bezeichnen sind, die neben Bitcoin am Markt koexistieren (Z. 131-142). Diese bringen technisch besser entwickelte Eigenschaften mit, um als Währung genutzt zu werden, da Geschwindigkeit und Transaktionskosten gegen Null gehen (ebd.). Einen technischen Vorteil sieht auch Fiedler (2017) nur in der alternativen Nutzung Bitcoins, welche dem Benutzer die komplette Kontrolle über sein Konto ermöglicht und Intermediäre überflüssig macht (ebd.).

Diese Eigenschaft hebt Dalal (2017), Technologie-Strategin der *Deloitte Consulting LLP* in Boston, besonders hervor (Z. 24-28). Die umfassende Kontrolle des Nutzers und das Wegfallen der Abhängigkeit von einer zentralen Entität und dem damit einhergehenden notwendigen Vertrauen in diese, sieht Dalal als wichtigen technischen Fortschritt an, der den Menschen die Möglichkeit einer mündigen Entscheidung bereitstellt, durch welche sie ihr Vertrauen auf ein weiteres System verteilen, und dadurch das Risiko des Verlustes des eigenen Vermögens durch Diversifizierung verringern können (2017, Z. 79-82). Dies zielt jedoch überwiegend auf den Aspekt der Wertspeicherung ab und weniger auf den des Einsatzes als Zahlungsmittel. Hierbei begreift auch Dalal (2017) Bitcoin nicht als skalierbares Netzwerk: „[…] in my opinion Bitcoin is not a network made for mass adoption in terms of a payment perspective." (Z. 88-90). Dalal sieht, wie alle Befragten, nur eine technisch konkurrenzfähige Nutzung als Zahlungsmittel in der Inanspruchnahme von Subsystemen, da Bitcoin alleine nicht in der Lage ist, technisch effizient als Zahlungsmittel eingesetzt zu werden und kein Potenzial birgt, dies durch eine Hardfork zu erreichen (ebd.).

Aus Sicht von Jeffries (2017), Autor für diverse Technologiemagazine und Blockchainentwickler, ist bei Bitcoin vor allem die systemimmanente Sicherheit und die Machtverteilung über das System hervorzuheben: „Consensus roles existed long before Blockchain. How much money is in supply in a centralized currency like the US Dollar or the Euro, their central banks set the rule. That is a consensus role on how much money being in circulation. They can change that rule without consulting anybody other than themselves whereas in Blockchain, because it is a protocol and math-based, the vast majority of people have got to agree to the change. So it makes changes slower, but it also makes sure that only the most important changes get through." (Z. 27-33). Hierbei identifiziert er einen weiteren Vorteil gegenüber souveränen Währungen, welche sich indirekt auf Bitcoin als Zahlungsmittel auswirken. Die technisch festgelegte Grenze von 21 Millionen schöpfbaren Bitcoin, erwirkt die deflationären Eigenschaften des Bitcoins. Zentralbanken können und werden fortlaufend ohne Zustimmung der Nutzer im System Geldeinheiten in gewünschter Höhe drucken (edb.). Dies führt zu einer Reihe von Vorteilen, wie dem Erreichen von Preisstabilität, auf lange Sicht jedoch

zu einer durchgehenden Inflation der Währung (ebd.). Jeffries (2017) sieht auch in der Konsensfindung einen größtmöglich demokratischen Ansatz, durch welchen der Markt Effizienzprobleme langsam, aber sicher lösen kann (Z. 24-41).

3.3.3. Ökonomische Effizienz

Übereinstimmung hinsichtlich der geringen ökonomischen Effizienz der Nutzung von Bitcoin als Zahlungsmittel mit dennoch vorherrschendem Potenzial wirtschaftlich effizient genutzt zu werden, ist bei sieben von acht Teilnehmern festzustellen.

Professor Ramb (2017) sieht die Dauer und Kosten der Transaktionen als systemimmanent an (53-54.). Die dadurch entstehenden Nachteile resultieren in einer unwirtschaftlichen Nutzung, können jedoch durch Subsysteme überwunden werden (Z. 54-64). Ramb (2017) zieht hierbei eine Analogie zum Bankensystem, in welcher er Bitcoin mit einer Zentralbank vergleicht und das Aufkommen von Subsystemen wie Privatbanken als natürlichen Prozess ansieht (ebd). Zum Zeitpunkt der Veröffentlichung dieser Arbeit ist das in der Entwicklung am weitesten fortgeschrittene Subsystem, das in Kapitel 2.2.4.3 dargestellte Lightning-Network, welches, die Transaktionen Off-Chain realisiert und später wieder in die Blockchain Bitcoins einspeist. Dies gehört, wie beschrieben, nicht zum Bitcoinsystem selbst und stellt einen zentralisierten Drittanbieterservice dar, der die Nutzung des Hauptsystems zu vereinfachen versucht. Sollte die Nachfrage nach Bitcoin als Zahlungsmittel steigen, so „würden sich automatisch dann Untersysteme bilden, die das lösen." (Z. 69-70).
Dennoch stellt vor allem die hohe Volatilität, welche seit Beginn einen kontinuierlichen Aufwärtstrend zu verzeichnen hat, eine starke Hemmschwelle für eine ökonomisch gerechtfertigte Nutzung als Zahlungsmittel dar, da eine „Preisungewissheit" besteht (Z. 159). „Bitcoin ist zwar volatil. Der Kurs bricht auch mal um 10%/20% ein, aber der langfristige Trend ist ganz eindeutig." (Z. 69-70). Dies ist auf das deflationäre System des Bitcoins zurückzuführen, welches das Halten von Bitcoin, in der Hoffnung auf Wertsteigerung, verursacht (ebd.). Diese Funktion der Wertspeicherung und Wertvermehrung steht der Nutzung als Zahlungsmittel maßgeblich gegenüber und erweist sich laut Ramb (2017) als der klügere Nutzen (ebd.). Einzig in Währungssystemen, in denen die Währung eine höhere Volatilität aufweist als Bitcoin selbst, kann eine wirtschaftlich vorteilhafte Nutzung erreicht werden (ebd.). Diese Räume zu identifizieren und die Chancen und Risiken der Nutzung von Bitcoin in stark volatilen Währungssystemen zu erforschen, geht jedoch über den Scope dieser Arbeit hinaus und ist in einer anknüpfenden Forschung zu bearbeiten.
Genau wie Ramb sieht auch Heller (2017) geringe Chancen in einer profitablen Etablierung Bitcoins als Zahlungsmittel ohne die Nutzung von Subsystemen (Z. 84 ff).

Studien zeigen, dass „niemand Bitcoins verkauft, auch da wo man es brauchen könnte, wird es nicht eingesetzt“ (Z. 68-69). Durch Transaktionskosten und langen Transaktionszeiten der Blockchain ohne die Nutzung von Drittanbietern, deren Sicherheit sich erst bewähren muss, „wird es niemals Sinn ergeben [...] einen Kaffee bei Starbucks mit Bitcoin zu bezahlen.“ (Z. 131-132).
Auch Fiedler (2017) kann in der Nutzung als Handelsmedium im Alltag der Bürger keinen ökonomischen Vorteil identifizieren: „Wenn ich mir ein Produkt damit kaufen möchte, dann möchte ich ungefähr vorher wissen, was ich für dieses Produkt ausgebe. Und wenn ich immer vorher nachschauen muss und eventuell feststelle, dass mein Produkt in den letzten 10 Minuten 10 Euro teurer geworden ist, dann würde ich das im Endeffekt als Nutzer nicht positiv sehen.“ (Z. 326-330). Durch die Volatilität leidet dementsprechend nicht nur der wirtschaftliche Einsatz als Zahlungsmittel, es entstehen auch enorme Preisschwankungen auf Seiten der zu erwerbenden Dienstleistung oder des Produktes (ebd.).
Kirschbaum (2017) identifiziert hierbei weitere wirtschaftliche Nachteile in der Verwendung von Bitcoin als Zahlungsmittel auf der steuerrechtlichen Seite, hervorgerufen durch die Volatilität (Z. 126 ff). Sobald der Besitzer von Bitcoins einen Wertgewinn zu verzeichnen hat, gilt es diesen nach deutschem Recht bei Ausgabe zu versteuern (ebd.). Dies stellt einen „buchhalterischen Alptraum“ (Kirschbaum, 2017, Z. 112) dar, weswegen die mit der Nutzung von Bitcoin als Zahlungsmittel einhergehende Bürokratie gegen dessen Nutzung als solches spricht (ebd.). Der Nutzer muss bei Ausgabe daher nachrechnen, wann er diesen Bitcoin gekauft hat, wann er ihn getauscht hat, und wie viel Steuern er daher an das Finanzamt zu entrichten hat (ebd.). Auch auf der Händlerseite ergeben zusätzliche Schritte im Vergleich zur Nutzung einer souveränen Staatswährung. Nimmt der Händler eine Zahlung in Bitcoin an, so muss die zu zahlende Umsatzsteuer dennoch in Euro an das Finanzamt übergeben werden, da dieses nur die staatliche Währung des europäischen Raumes akzeptiert (ebd.). Der Händler muss also, wenn er durch weitere Geschäfte nicht auch genügend Euro einnimmt, um diese an das Finanzamt weiterzuleiten, die Bitcoin vorerst in Euro umtauschen, was „wiederrum ein steuerpflichtiger Vorgang sein kann, wenn Wertsteigerung oder Wertsenkung realisiert worden sind.“ (Z. 177-187).

Auf die weiterführende Frage nach der Einschätzung der aktuellen Akzeptanz des Bitcoins als Zahlungsmittel am Markt lässt sich Übereinstimmung in den Aussagen von Kirschbaum und Fiedler wiederfinden. Fiedler (2017) sind dabei nur sehr wenige Unternehmen bekannt, die eine Zahlung mit Bitcoin offerieren (Z. 376-381). Das Anbieten oder öffentliche Nachdenken diese Methode der Zahlung auf der eigenen Plattform einzuführen, begreift Fiedler (2017) als „[...] Marketinggag, vor allem auf-

grund der genannten Transaktionsgebühren und -zeiten.“ (Z. 380-386). Auch Kirschbaum (2017) geht deckungsgleich von diesem Beweggrund der Unternehmen aus: „Die meisten Unternehmen, die jetzt Bitcoin als Zahlungsmittel angenommen haben, [...] haben das glaube ich eher aus Marketinggründen gemacht, als daraus, dass sie wirklich einen Vorteil darin gesehen haben, Bitcoin als Zahlungsmittel einzuführen.“ (Z. 68-71).

Ähnlichkeit hinsichtlich der Aussagen lässt sich bei Charrier feststellen. Die Akzeptanz ist zwar noch sehr gering, wird sich aber in absehbarer Zeit in bestimmten Nischen erhöhen (Charrier, 2017, Z. 298-300). Anzeichen für die hohe Wahrscheinlichkeit seiner Aussage identifiziert Charrier (2017) in dem Aufkommen von mehr und mehr Kryptomillionären, die ihr Geld nicht zwangsweise über Börsen liquidieren möchten: „[...] die wollen ja auch etwas mit ihrem Geld machen und das wissen ja natürlich auch die Unternehmen. Ich sehe vielleicht einen großen Bereich in Luxusgütern, dass vielleicht ein Tesla bald mit Bitcoin gekauft werden kann, oder Gucci.“ (Z. 293-300). Die Bezahlung mit Bitcoin wird daher erst einmal eine Art „Elite Status“ (Charrier, 2017, Z. 295) darstellen, welcher sich „langsam nach unten fortsetzen und eine große Akzeptanz finden [wird].“ (ebd.).

Die weiteren Experten begreifen die Akzeptanz Bitcoins als Zahlungsmittel am Markt als ähnlich gering und führen dies überwiegend auf die bereits identifizierten hohen Kosten und langen Zeiten der Transaktionen zurück (et al.). Bis auf Kirschbaum und Fiedler stufen diese ihren Wissensschatz hinsichtlich der Frage jedoch nicht als ausreichend fundiert ein, um eine aussagekräftige Antwort bezüglich der Frage anbieten zu können (et al.).

3.3.4. Systemsicherheit und Usability

Übereinstimmung hinsichtlich der Frage nach der Sicherheit der Nutzung von Bitcoin als Zahlungsmittel, sowie der Usability selbst findet sich, wie auch schon bei den vorigen Kategorien, bei der überwiegenden Anzahl der Experten wieder.

Nigischer und Kirschbaum teilen die Meinung, dass die Risiken vor allem in der unausgereiften Usability der Wallets existieren. Kirschbaum (2017) begreift die fehleranfällige Usability dabei als kontextuell durch den Ursprung Bitcoins geprägt, welcher auf Programmierern mit der Ideologie beruht, Banken obsolet zu machen: „Da steht dann die Usability für den Endkunden in der Programmierung ziemlich weit hinten.“ (Z. 299-300) (ebd.). Vertippt sich ein Nutzer in der Adresseingabe oder macht einen Fehler im Kopieren der Adresse, so sendet er seine Bitcoins an eine falsche Adresse,

wobei keine Möglichkeit besteht, die Bitcoins zurückzuholen (Nigischer, 2017, Z. 39-47). Das Fehlen von Prüfmechanismen für eine Korrektheit der Adresseingabe in den Wallets, verstärkt dieses Problem (ebd.). In einer korrekten und sorgfältigen Nutzung der Core-Wallets sieht Nigischer allerdings kein Problem (2017, ebd.). Diese systemimmanenten Eigenschaften erfordern eine andere Handhabe und ein vermehrtes Nachdenken als die Nutzung von gewohnten Zahlungssystemen wie Visa oder PayPal (Nigischer, 2017, Z. 58-62).

Diesbezügliche Übereinstimmung ist hierbei bei Fiedler und Ramb zu finden. Ramb (2017) begreift die Unumkehrbarkeit einer Transaktion neben einem Risiko auch als inhärent: „[...] jeder Nutzer des Bitcoins kennt diese Spielregel und muss sich entsprechend darauf einstellen, und wenn er sich vertut, hat er sich vertan. Dann ist das Geld halt weg, aber ohne dieses Risiko gibt es kein Bitcoin." (Z. 38-41). Laut Fiedler (2017) gilt es, bei dem Thema Sicherheit und Usability zusätzlich zwischen Unternehmen und privaten Nutzern zu differenzieren. Unternehmen können nach einer Schulung sehr wahrscheinlich professionell mit der Technologie umgehen und beispielsweise ein „gewisses IT-System von *SAP*" (Fiedler, 2017, Z. 344) nutzen, um die Sicherheit des Umganges mit großen Handelswährungen wie Bitcoin maßgeblich zu erhöhen (ebd.). Private Nutzer müssen jedoch eine „gewisse technische Affinität" (Fiedler, 2017, Z. 346-348) mit sich bringen, was einer Nutzung als Zahlungsmittel durch die breite Masse als Hemmschwelle im Weg steht (ebd.; Ramb, 2017, Z. 241-260). Fiedler (2017) bezieht sich dabei auch auf sein Bankerumfeld, in welchem viele „es für sehr sinnvoll halten, aus Spekulationsgründen ein paar Bitcoin zu kaufen, es aber niemals umgesetzt haben" (Z. 348-351). Dies führt Fiedler (2017) durch die Gespräche mit diesen auf die genannte Hemmschwelle bezüglich des benötigten technischen Verständnisses zurück, die nur mit einer gewissen zeitintensiven Einarbeitung in das Thema oder einer Vereinfachung des Kauf- und Sicherungsprozesses der Bitcoin überwunden werden kann[51] (ebd.). Hierbei spricht Fiedler auch dem Aufkommen von Drittanbietern, die diese Hürden zu senken versuchen, viel Potenzial zu. Als Beispiel nennt Fiedler (2017) die Bank *Vontobel*, welche für den Kunden den Erwerb und die Speicherung der Bitcoin auf einem Hardwarewallet, sowie dessen sichere Lagerung im Tresor übernimmt (Z. 345-362).

Weiterführend sollte laut Fiedler bei der Sicherheit der Blockchain klar zwischen der Systemsicherheit und der Sicherheit der individuellen Nutzung unterschieden werden.

[51] Der Autor hat sich entschieden diesen Aspekt als Beispiel für das Aufkommen von Drittanbietern miteinzubeziehen, obwohl sich die Nutzung von Bitcoin als Spekulations- und/oder Wertspeicherungsobjekt nicht direkt auf die Leitfragestellung dieser Arbeit bezieht.

Die Blockchain-Technologie selbst ist als extrem sicher einzustufen (Fiedler, 2017, Z. 340-342). Aus einem Hash kann das Passwort nur theoretisch wieder umgewandelt werden, wobei sich ein solches Unterfangen nicht unter vernünftigem Aufwand realisieren lässt: „Das wird für Hacker immer irrational bleiben [...]." (Fiedler, 2017, Z. 72). Der Nutzer läuft jedoch in der individuellen Nutzung des Systems durch Wallets Gefahr, beispielsweise sein Paper-Wallet oder sein Hardwarewallet, welches die Sammlung aller Keys beinhaltet, zu verlieren oder beraubt zu werden (ebd.). Bei einer korrekten und sicheren Nutzung der Wallets sieht jedoch auch Fiedler keine Gefahr (2017, ebd.). Allerdings stuft Fiedler die Anlaufstellen, an denen der Bitcoin umgetauscht oder liquidiert werden kann, die Börsen, als besonders unsicher ein (edb.). Fiedler bezieht sich dabei auf Hacks wie bei *Mt. Gox*[52] und Bitfinex[53], durch welche Bitcoin in Millionenhöhe entwendet werden konnten (ebd.). Diese können jedoch an den meisten Börsen nicht mehr liquidiert werden, da die Adressen, auf die die gestohlenen Bitcoins eingegangen sind, durch die Transparenz des Netzwerkes bekannt sind und von den Börsen daher auf einer schwarzen Liste aufgeführt wurden. Lediglich bei bestimmten Anbietern, die diese Adressen nicht gelistet haben, könnten die gestohlenen Bitcoin eventuell unbemerkt als Zahlungsmittel genutzt werden (Fiedler, 2017, Z. 83). Fiedler (2017) geht jedoch davon aus, dass die Hacker mit diesem Angriff keinen reinen Diebstahl im Fokus hatten, sondern auf einen, durch die Presse-Nachrichten des Hacks ausgelösten, Fall des Bitcoin-Börsenkurses spekuliert haben, um von diesem zu profitieren (Z. 82-93).

Ein weiteres Risiko identifiziert Dalal (2017) bei der Nutzung von Bitcoin als Zahlungsmittel in dem Fehlen von Governance, also einer zentralen Steuerung (Z. 69-73). Das Fehlen der Möglichkeit, eine Zahlung an die falsche Adresse rückgängig zu machen, sieht Dalal dabei kritischer als Fiedler und Nigischer (2017, Z. 37-40). Auch in der identifizierten Chance, die volle Verfügung als Nutzer über das eigene Konto ohne die Abhängigkeit von Intermediären zu haben, sieht Dalal ein großes Sicherheitsrisiko (ebd.). Wird Bitcoin im Alltag als Handelsmedium genutzt, so ist der User durchgehend

[52] Bei Mt. Gox handelte es sich 2013 um die größte Bitcoinbörse, die in dem genannten Jahr 60% des weltweiten Handelsvolumen von Bitcoin zu verzeichnen hatte. 2011 wurden dieser durch einen Hack Bitcoin im damaligen Wert von 8,75 Millionen Dollar entwendet. Nach zahlreichen weiteren zwielichtigen Aktivitäten seitens der Börse und darauffolgenden Klagen durch die Nutzer meldete Mt. Gox im Februar 2014 Insolvenz an, wobei viele Nutzer nie ausgezahlt wurden. Im August 2015 wurde der frühere Chef von Mt. Gox von den japanischen Behörden festgenommen und bezichtigt, zum eigenen Vorteil in das System der Börse eingegriffen zu haben (Mick, 2011; Mt. Gox, 2014; dpa, 2015).

[53] Die Börse Bitfinex wurde zwei Mal Opfer eines Angriffs. Im August 2016 entwendeten Hacker 122.000 Bitcoin im damaligen Wert von 72 Millionen Dollar und im Dezember 2017 erreichten Hacker eine Lahmlegung der Webseite, welche mehrere Stunden andauerte und alle Nutzer am Zugriff auf die eigenen Konten hinderte. Die geschädigten Kunden der Börse erhielten jedoch Schadensersatz, welche auch heute noch als eine der größte Krypto-Börsen am Markt besteht (Reuters, 2017).

der Gefahr eines Hackerangriffs auf sein Smartphone oder seinen Computer ausgesetzt, sofern er keine Paper-, oder Hardware-Wallets nutzt, welche sich, vor allem außerhalb des Wohnraumes, als sehr unhandlich erweisen würden (ebd.). Im Falle eines erfolgreichen Angriffs haftet daher kein Intermediär wie eine Bank, die für den Verlust oder das Durchbrechen der Sicherheit aufkommt (Dalal, 2017, Z. 55-62). Ähnlich wie bei Ramb und Fiedler ist auch bei Dalal (2017) eine Übereinstimmung hinsichtlich des nötigen Lernprozesses bei der Nutzung der neuen Technologie in Unternehmen festzustellen: „I think this is more of a feature that people will have to adapt to. When we are talking about not being able to reverse the transaction, we are talking about a human error in that it got send to the wrong address. People in companies will have to be schooled to learn the skills and I believe this will work fine." (ebd.). Auch für den privaten Anwender sieht Dalal, in der aktuellen Ausprägung der Technologie eine große technische Barriere (ebd.). In dem Voranschreiten dieser und der Adaption auf Smartphones bestehen jedoch weitaus größere Chancen, dass Bitcoin ohne technische Verständnishürden von der Masse als Zahlungsmittel genutzt werden kann (Dalal, 2017, Z. 79-82).

Übereinstimmungen bezüglich der Frage nach der Sicherheit von Proof-of-Work sind bei Heller, Kirschbaum und Jeffries zu finden, da diese Experten die Sicherheit in der Bewährtheit des Systems thematisieren.

Heller (2017) sieht in dem Proof-of-Work Konzept eine einfache und bewährte Sicherheitsmaßnahme, die zur Fairness und ansatzweisen Demokratie in dem System beiträgt (Z. 151-157). Proof-of-Work ermöglicht eine energiegebundene Sicherheit, die dadurch schwer anzugreifen ist (ebd.). Auch angesichts der voranschreitenden Zentralisierung der Mining-Pools sieht Heller (2017) Bitcoin keiner akuten Gefahr ausgesetzt: „Die Wahrscheinlichkeit einer 51%-Attacke nimmt mit dem Steigen des Preises ab." (Z. 151-152). Kirschbaum betrachtet die Sicherheit des Systems ebenfalls als gegeben und sieht vor allem in der Transparenz des Netzwerkes einen großen Vorteil. Sollte es Miner oder Mining-Pools geben, die einen solchen Angriff durchführen, so könnten diese leicht identifiziert werden (Kirschbaum, 2017, Z. 316-323). Eine solche Übernahme könnte auch nur für Double-Spending oder das Ablehnen von Transaktionen genutzt werden, was sich nicht als wirtschaftlich erweisen würde (ebd.). PoW benötigt jedoch enorm viel Energie und stellt durch das ansteigende Wachstum des Systems eine immer größere Herausforderung dar und beginnt, angesichts der Größe auch eine Belastung für die Umwelt zu werden (Kirschbaum, 2017, Z. 327-338). Als Alternative sehen Heller, Kirschbaum und Jeffries

dabei Proof-of-Stake[54] (2017, et al.). Jeffries (2017) stellt bei Proof-of-Work und Proof-of-Stake eine Analogie zwischen analogen und digitalen Bremsen bei Autos her: „Analog breaking was basically a couple of moving parts, and we developed a way for them to work pretty much flawlessly every single time. Whereas digital breaks introduced a number of vulnerabilities [...].“ (Z. 305-309). PoW ist ein einfaches, aber effektives und leicht nachvollziehbares Konzept, bei welchem die möglichen Fehler überschaubar und begrenzt sind (Z. 301-303). PoS muss sich, trotz theoretischer Vorteile, noch bewähren und die vielen möglichen Fehler und Angriffsflächen in der Entwicklung beseitigen (Jeffries, 2017, Z. 310-318.).

3.3.5. Stabilität des Ökosystems

Um Bitcoin als Zahlungsmittel gefahrenfrei nutzen zu können, muss das geschaffene Ökosystem als stabil einzustufen sein. Zwecks Begutachtung der Technologie und ihrer äußeren Einflüsse, bedarf es daher einer Analyse des Ökosystems der direkten Teilhaber des Systems. Hierzu zählen die Miner, die Nodebetreiber, die Entwickler und die Nutzer. Diese Kräfte haben den größten Einfluss auf den Fortbestand, die Stabilität und die Richtungsentwicklung der Technologie.

Übereinstimmung hinsichtlich der Frage nach der Stabilität des Ökosystems lässt sich, bezogen auf das Thema *Governance* bei Nigischer, Jeffries, Fiedler, Dalal und Ramb aufgrund der Aussagen finden, dass hierbei Chancen durch die Regelung des Marktes und Risiken durch die geringe Anzahl der Beteiligten, welche an der direkten Aufrechterhaltung und Weiterentwicklung des Systems mitwirken, entstehen. Nigischer (2017) erkennt in dem kleinen, elitären Kreis der Entwickler, Miner und Nodebetreiber, welche die Eigenschaften des Systems maßgeblich formen, ein mögliches Systemrisiko (Z. 100-106). Würde dieser kleine Kreis gegen die Erwartungen und/oder Sicherheitsanforderungen der Nutzer agieren, so wäre dies „auf jeden Fall problematisch“ (ebd.). Sollte der Eindruck entstehen, dass dort „Schindluder getrieben wird, und dass das von wenigen wissenden und mächtigen ausgenutzt wird, dann kann das einen erheblichen Schaden für die langfristige Entwicklung nach sich ziehen.“ (Nigischer, 2017, Z. 256-259). Der überschaubare Kern des Systems bedeutet für Nigischer: „Fragilität ist durchaus auch vorhanden“ (Z. 106). Dennoch stellt Nigischer gegenüber, dass trotz

[54] Bei Proof-of-Stake (PoS) handelt es sich um eine alternative Methode Transaktionen zu bestätigen. Diese Methode macht Miner überflüssig, da Teilnehmer des Systems über die Full/Light-Nodes eine bestimmte Anzahl an Coins für einen festgelegten Zeitraum einschließen können. Diese Coins können dann nicht mehr berührt werden und bestimmten prozentual zu den weiteren *gestakten* Coins die Wahrscheinlichkeit, dass die eigene Node eine Transaktion bestätigen darf. Ist dies der Fall, so erhält der stakende den Reward. Diese, bei Bitcoin noch nicht geplante, Methode ist jedoch weitaus komplexer als PoW und bedarf noch vielen Tests (Morabito, S. 32).

vorherrschender Meinungsverschiedenheiten, bezogen auf die Hard-Forks, alle Teilnehmer am Markt ein Interesse an einem sicheren Bestand von Bitcoin haben, da diese dabei die größten Vorteile daraus ziehen (ebd.). Auch Dalal (2017) sieht in der Abhängigkeit von einem kleinen Kreis eine mögliche Gefahr der Stabilität, stuft Bitcoin jedoch als stabil ein: „When you have a public blockchain, such as bitcoin, it is about the number of people who control the development – like with bitcoin core or bitcoin cash. It is a very small group, yet bitcoin has proven to be very stable." (Z. 69-73).
Kirschbaum (2017) begreift die alleinige Regelung durch den Markt ebenfalls eher als Chance, denn als Risiko: „Gerade weil sich der Preis von Bitcoin am Markt bestimmen muss, ist die Preisfindung ja den kapitalistischen Kräften ausgesetzt [...]." (Z. 138-141). Dies stellt einen Vorteil und eine Chance gegenüber staatlichen Währungen dar, da die geldausgebenden Instanzen der Staaten nicht nur im Hinblick auf die nationalen geldpolitischen Interessen agieren, sondern auch Entscheidungen hinsichtlich internationaler (geld-)politischer Interessen vertreten, welche der landeseigenen Währung nicht zwingend zum größtmöglichen Vorteil dienen (Kirschbaum, 2017, Z. ebd.). Chancen ergeben sich auch durch die Hardforks, welche laut Jeffries (2017) als sehr gesund für das Ökosystem einzustufen sind. Diese tragen demokratische Fairness zum Thema Governance bei und eröffnen die Möglichkeit, den Markt selbst das richtige Produkt formen zu lassen: „The only way to solve that is to do Darwin in economics and through competition through those Hard Forks. I see that as a way to resolve those political differences." (Z. 173-175). Für Jeffries ergeben sich durch die Forks vor allem auch langfristige Chancen für die Stabilität des dezentralen Bitcoins gegenüber einer zentralen Währung. Jeffries (2017) beschreibt *Vertrauen* dabei als dynamisch: „Trust is a moving concept, it is not a fixed concept. People mistakenly understand trust as a fixed concept, it is never, it is moving all times." (Z. 348-349). In diesem Zusammenhang führt Jeffries (2017) ein chinesisches Sprichwort an: „[...] when the price of rice is high, heaven decrees new rulers." (Z. 362-363). Wird ein Unternehmen oder ein Staat jahrelang gut geführt, bedeutet dies nicht, dass die Wahl der falschen Machthaber nicht zu einem Verlust von Vertrauen führen kann: „Evansville[55] is a perfect example of a country. There was a thriving economy that was looking to break out of banana republic status into becoming a real power house and got the wrong people in charge and suddenly crashed the economy and people are starving." (Z. 354-357). Jeffries (2017) zieht hierbei eine Parallele zu dem Unterschied dezentraler und zentraler Konsensfindung. Der Vorteil eines Systems, in dem der Konsens zur Entscheidungsfindung dezentral geregelt wird, liegt in seiner Machtverteilung (ebd.). Eine zentrale Institution ist aufgrund der zentralen und vergleichsweise kleingruppigen Steuerung weitaus fragiler als das dezentrale Bitcoin-System (ebd.).

[55] Eine Stadt in Indiana in den Vereinigten Staaten von Amerika.

Jeffries (2017) geht weiterführend darauf ein, dass ein dezentrales System wie Bitcoin auch das historische Problem sogenannter „soft promises“ (Z. 153-155) löst (ebd.). Unter *soft promises* versteht Jeffries (2017) Versprechen, die Staaten oder Politiker dem Volk, vor allem in Wahlkämpfen geben, welche überwiegend nicht eingehalten werden und auch gesetzlich nicht eingehalten werden müssen (ebd.). Unter Bitcoin kann daher ein System verstanden werden, welches durch seine mathematisch und technisch festgelegten Regeln und die Endlichkeit der Einheiten nicht brechbare „hard promises“ (ebd.) bietet, auf die sich der Nutzer verlassen kann (ebd.). Hinzu kommt der globale Aspekt, welcher laut Jeffries (2017) mit zunehmendem Wachstum eine exponentielle Steigerung der Systemstabilität zur Folge hat: „Overtime, I see a protocol where everyone has a stake in it being valuable, even people who disagree from the Russians and United States and Venezuela. All potentially have a stake in Bitcoin being profitable […]. Then I believe that that is more powerful than a single nation state which could put in the wrong people. It's less likely that all of the nation states would simultaneously go bad in the world and destroy a truly decentralized currency that is ubiquitous and widely used.” (Z. 368-270). Jeffries begreift es als logische Schlussfolgerung, dass eine Währung, die nur von einem Staat gestützt wird, weitaus instabiler ist als eine dezentrale Währung, an deren Stabilität der gesamte Weltmarkt ein Interesse hat (ebd.).

Auch Ramb (2017) beurteilt das Interesse des Marktes als maßgeblichen Faktor für die Stabilität des Bitcoins und arbeitet hinsichtlich der Frage nach der Stabilität mit einer Analogie zur Gründung der USA und der Entwicklung des heutigen Dollars:

> „Da gab es auch ein halbes Dutzend Währungen, ein halbes Dutzend Dollarvarianten, die zum großen Teil zusammengebrochen sind, die zum großen Teil einzelnen Regionalbanken zugewiesen waren, die dann ausgeraubt wurden oder was weiß ich auch immer. Auf die Dauer hat sich das dann in, wenn Sie so wollen, darwinistischer oder ich sage dann auch immer im Sinne der ökonomischen Effizienz herausgestellt, ein starkes System, und diese Situation werden wir im Bitcoin auch haben. Es gibt die Derivate, es gibt die Subsysteme, die miteinander konkurrieren. Die schlechten Werte werden vom Markt verschwinden. Die guten werden überleben, aber überleben werden auf jeden Fall einige Systeme.“ (Z. 114-122).

Ramb (2017) merkt hierbei an, dass vor allem durch das Aufkommen von Subsystemen mögliche Stabilitätshindernisse, wie die technisch systemimmanenten, hohen Transaktionskosten abgefangen werden können (Z. 195-198). Des Weiteren sieht Ramb (2017) wie Jeffries einen exponentiellen Anstieg der Stabilität in dem Wachstum der Attraktivität, welche durch die Vereinfachung der Nutzung der Technologie durch eben diese Subsysteme gravierend beeinflusst wird (ebd.). Diese tragen dazu bei, dass das Risiko eines Kurseinbruchs mit der Zunahme der Nutz- und

Greifbarkeit Bitcoins durch die Vereinfachung für den Endnutzer maßgeblich gesenkt wird (Ramb, 2017, Z. 260). Als Gegenbeispiel führt Ramb (2017) die Milchmädchen Hausse[56] an (Z. 242-255). Da aber Bitcoin als Technologie jedoch durch den Markt mehr Anwendung im Alltag erfahren könnte, sieht Ramb (2017) eben diese Gefahr als weniger wahrscheinlich (Z. 250-260).
Ein leichtes Risiko identifiziert Fiedler (2017) in den wenig regulierten und oft schlecht funktionierenden Krypto-Börsen (ebd.). Der Handel von Bitcoin ist „lange nicht so ausgereift, wie der Handel von anderen Währungen, wie dem Dollar, dem Euro oder Rohstoffen usw. Aber weil der Handel noch so in den Kinderschuhen steckt, sind dort dementsprechend auch noch viele Risiken drin." (Fiedler, 2017, Z. 81-83). Eines dieser Risiken stellt eine mögliche Marktmanipulation dar, welche angesichts der, im Vergleich zu staatlichen Währungen, geringen Marktkapitalisierung Bitcoins, noch von Händlern mit großen Volumina leichter durchgeführt werden kann: „Teilweise machen die Kurse Sprünge nach oben oder nach unten, die völlig irrational erscheinen. Da ist davon auszugehen, dass diejenigen ihre Marktmacht missbrauchen um bei einem sehr kleinen Order-Buch dort mit Insider-Informationen sehr viel Geld verdienen. Das ist auf klassischen Finanzmärkten ganz klar reguliert. Dafür kommt man ins Gefängnis, falls man Derartiges tut." (Fiedler, 2017, Z. 437-438). Allerdings ist dies bei Bitcoin durch den enormen Anstieg der Markkapitalisierung[57] immer weniger der Fall und stellt eher eine Gefahr für alternative Krypto-Assets dar (ebd.).

Bei den Aussagen Fiedlers und Hellers ist eine Ähnlichkeit hinsichtlich der Frage nach dem Beitrag der Hard-Forks zur Stabilität zu erkennen. Fiedler (2017) sieht die Hard-Forks als kritischer an und identifiziert eine Unsicherheit in diesen, die zu einer Verwirrung von Außenstehenden führen können (Z. 176-178). Ein wirkliches Risiko besteht aufgrund der zu beobachtenden Stabilität nach diesen jedoch nicht (Fiedler, 2017, Z. 81-82). Auch Heller (2017) sieht in den Forks neben Chancen auch Risiken: „Auf eine Art ist es ja nicht schlecht, wie Konsens in dem System gefunden wird. Aber jede Fork ist ein Eingeständnis, dass man einen Fehler in der Vergangenheit gemacht hat." (Z. 142-144). Das System muss noch reifen und bietet zwar durch die Forks das Potenzial einer soliden Stabilität, ist jedoch aktuell noch fragil (ebd.). Dennoch merkt Heller an, dass er das System der Forks für sinnvoll hält und „[...] eine Sympathie für die Art, wie es umgesetzt wird." (Z. 145-146) empfindet (ebd.).

---

[56] Als Milchmädchen Hausse wird an der Börse die Endphase eines starken mittel- langfristigen Aufwärtstrends einer Aktie bezeichnet, in der auch die breite Bevölkerungsschicht, die sonst nicht in diesem Markt agiert, in der Hoffnung auf weitere Wertgewinne in diese Aktie investiert (Börsenlexikon, 2008).
[57] Marktkapitalisierung Bitcoins: 16.755.375 BTC. Bei einem Kurs von 17.635$/BTC entspricht dies 295.492.060.000$ [20.12.2017; 00:00 Uhr] (Coingecko, 2017; Xe, 2017)

3.3.6. Gesetzliche Einflussfaktoren

Der Einschätzung von Kirschbaum (2017) zufolge ist Bitcoin in der Nutzung als Zahlungsmittel im deutschen Raum bereits steuer- und finanzrechtlich durch die entsprechenden Gesetze fast vollends reguliert. Bezogen auf die Nutzung als Zahlungsmittel gilt es, Wertzuwächse zu versteuern: „Sie haben natürlich [...] das Problem, wenn die Bitcoins, die Sie nutzen, um die Ware zu kaufen, zwischenzeitig im Wert gestiegen oder gefallen sind [...] eventuell einen steuerwirksamen Vorgang." (Z. 178-183). Dadurch gilt es in diesem Fall „nicht nur die Ware, die Sie jetzt bekommen haben, zu bezahlen, sondern auch noch eventuell Steuern für die Wertsteigerung an das Finanzamt [zu entrichten]." (ebd.). Auf der Händlerseite muss das Unternehmen die Umsatzsteuer an das Finanzamt in Euro zahlen und ist somit angehalten, entweder durch Verkäufe Euro in entsprechender Höhe einzunehmen, oder die Bitcoins in Euro umzutauschen, „was wiederrum ein steuerpflichtiger Vorgang sein kann, wenn Wertsteigerung oder Wertsenkung realisiert worden sind." (Z. 185-187; EStG, 2018[58]). Auch die Börsen begreift Kirschbaum (2017) im deutschen Raum als reguliert: „Da die BaFin[59] Bitcoin und andere Kryptowährungseinheiten als Recheneinheiten und damit als Finanzinstrumente im Sinne des Kreditwesengesetzes eingestuft hat, ist ja quasi jeder, der in größeren Mengen mit Kryptowährungen handelt, oder einen Marktplatz anbietet [...] immer [in] Gefahr, von der BaFin als Finanzdienstleistungsunternehmen eingestuft zu werden und deswegen eine BaFin-Erlaubnis zu brauchen." (Z. 367-372). Kirschbaum (2017) stuft diese Gesetzgebung als hinderlich für die Entwicklung des deutschen Krypto-Marktes ein, welcher dadurch in der Unterstützung und Bildung von Subsystemen für Bitcoins als gehemmt anzusehen ist (ebd.). Er fügt hinzu, dass man schauen müsse, ob man „Kryptowährungen nicht aus der Banken- und Finanzdienstleistung herausnimmt und ein eigenes Regelwerk schafft, das vielleicht ein bisschen Start-Up freundlicher ist, als das starre Bankensystem, das ja eigentlich für ganz andere Anwendungsfälle konstruiert worden ist." (ebd.). Dies bezieht sich jedoch nur auf den deutschen Raum. Als kompliziert stuft Kirschbaum (2017) die verbraucherschutzrechtlichen Regelungen zur Rückerstattung eines Betrages in Bitcoins nach Wertanstieg oder -senkung im Vergleich zum Euro ein. Kauft ein Kunde ein Produkt zu einem Preis von Bitcoins mit Kurswert von 300 €, und dieser liefert defekte Ware, so kann der Verkäufer „unter denselben verbraucherschutzrechtlichen Regelungen wie beim Kauf mit Euro verklagt werden" (Z. 165-166) und ist verpflichtet, den Kaufpreis [in

---

[58] Den Wertgewinn, der bei einer Veräußerung erzielt wird, gilt es zu versteuern. Für Privatanleger findet sich die entsprechende Vorschrift in § 23 Abs. 1 Nr. 2 EStG. Gewerbetreibende ermitteln den Gewinn über Einnahme-Überschuss-Rechnung (§ 4 Abs. 3 EStG) beziehungsweise über Betriebsvermögensvergleich (§ 5 Abs. 1 EStG) was grundsätzlich zu denselben Ergebnissen führen sollte (Einkommenssteuergesetz, 2018).

[59] Die Bundesanstalt für Finanzdienstleistungsaufsicht hat die Aufgabe der Kontrolle und der Beaufsichtigung aller Bereiche des Finanzwesens in Deutschland (BaFin, 2014).

Bitcoins] zurückzuzahlen“ (ebd.). Dabei erfordert § 355 Abs. 3 BGB die Rückgewähr in Natur. Das bedeutet laut Kirschbaum (2017), dass die Bitcoins, unabhängig vom veränderten Kurswert zurückerstattet werden müssen. Verbraucher tragen somit ein gewisses Risiko, dass die Ausübung des Widerrufsrechts mit einem Wertverlust einhergeht. Andererseits trägt der Händler ein Risiko, dass der Verbraucher sein Widerrufsrecht – dass ja generell nicht begründet werden braucht – ausübt, wenn Bitcoins im Wert gestiegen sind, einfach um den Wertzuwachs zu realisieren und die erworbene Ware dann eben erneut zu kaufen (ebd.).
Neben den genannten rechtlichen Begebenheiten und möglichen Risiken kann Kirschbaum keine weiteren steuer- oder finanzrechtlichen Chancen in der Nutzung von Bitcoin als Zahlungsmittel erkennen.

Fiedler (2017) erkennt in der Transparenz des Netzwerks zusätzlich die Chance eines einfachen Nachweises einer getätigten Transaktion mit etwaigem Wertgewinn. Durch die Irreversibilität der Blockchains lassen sich die steuerwirksamen Vorgänge „nachträglich rekonstruieren und Gewinne oder Verluste aufzeigen.“ (Z. 309-311), auch wenn die eigenen Aufzeichnungen über Zahlungen und Geldeingänge abhandengekommen sind (ebd.). Ein Risiko besteht jedoch in der gesetzlichen Grauzone und dementsprechend fehlenden Verfolgung von Marktmanipulationen: „Streng genommen ist mir persönlich kein Gesetz bekannt, das Kryptowährungen verbietet. Da müssen aus meiner Sicht ganz klare Regeln her, die dazu führen, dass jeder weiß, was er tun darf. Außerdem muss eine Verfolgung stattfinden, damit die, die das ausnutzen, auch entsprechend bestraft werden können und am besten auch bestraft werden, um andere abzuschrecken. Das ist ein weiteres Zeichen für dieses sehr frühe Marktstadium des Kryptotradings.“ (Fiedler, 2017, Z. 550-555). Diese Grauzone stellt aktuell ein kleines Risiko durch die verursachte Volatilität dar, schadet jedoch eher kleineren Krypto-Assets mit einer weitaus geringeren Marktkapitalisierung, in der eine Manipulation angesichts dieser weitaus einfach umzusetzen ist (Fiedler, 2017, Z. 425-428). Im Rahmen der Besteuerung der Wertgewinne sieht Heller (2017) eine Chance auf Seiten des Staates, der das momentane Risiko trägt, Wertgewinne nicht nachverfolgen zu können (Z. 191-194). Dieser muss die internationalen Regeln für Wertgewinne nur noch auf die Börsen übertragen: „Es ist einfach die Implementierung, die noch nicht erfolgt ist. In den USA wissen die wer ich bin, Coinbase[60] weiß wer ich bin. Die können das an sich auch dem Finanzamt weitergeben.“ (Heller, 2017, Z. 195).

[60] Die Kryptobörse Coinbase zählt seit ihrer Gründung im Jahre 2012 zu den größten Börsen am Markt (Bloomberg, 2012).

3.4. Zusammenfassung der Forschungsergebnisse

In der vorangegangenen Analyse wurde das hybride Krypto-Asset Bitcoin, im Hinblick auf die zu beantwortende Forschungsfrage, sowie die zu verifizierenden und/oder falsifizierenden (Hypo-) These(n) hinsichtlich sechs Aspekten betrachtet: Erstens, die technische Effizienz der Bitcoin-Technologie, zweitens, die ökonomische Effizienz einer Nutzung als Zahlungsmittel, drittens, die technische Sicherheit der Technologie sowie der Usability, viertens, die staatlichen Einflussfaktoren und fünftens, die Stabilität des Ökosystems.

Während die Blockchain-Technologie durch die Peer-to-Peer Lösung und den Wegfall von Intermediären theoretisch die Chance von Kostenersparnis bei der Transaktions-durchführung mit sich bringt, ist das System praktisch nicht auf eine Nutzung in der vorherrschenden Größenordnung ausgelegt. Die hohen Transaktionskosten und Transaktionszeiten sind auf ein Skalierungsproblem der Technologie zurückzuführen und ohne eine Nutzung von zentralen Subsystemen wie dem Lightning-Network nicht zu umgehen. Eine Konkurrenzfähigkeit gegenüber den herkömmlichen Zahlungsmitteln ist ohne die Inanspruchnahme dieser aufgrund der systemimmanenten technischen Eigenschaften nicht gegeben. Verglichen mit genannten herkömmlichen Zahlungsmitteln bietet Bitcoin daher aktuell keine Chancen gegenüber diesen in seiner Nutzung. Auch offenbart sich die Hürde, die Bitcoin-Zahlungssysteme noch am Point of Sale zu integrieren. Eine Nutzung der, bereits am Markt integrierten, Systeme ist dabei nicht möglich. Des Weiteren stellt der Zeitraum bis zur Unumkehrbarkeit der Zahlungen mit ungefähr einer Stunde eine, für viele Händler, inakzeptable Dauer dar. Effizienz gegenüber souveränen Währungen zeigt sich jedoch in den deflationären Eigenschaften Bitcoins, welche durch eine mathematisch und technisch festgelegte Schöpfung der Coins und die Endlichkeit dieser erreicht wird. Diese Chance bezieht sich jedoch nur auf die Eigenschaft der Wertspeicherung/Wertvermehrung. Das Proof-of-Work Systems ermöglicht im Zusammenspiel mit den Nodes ein hohes Maß an Sicherheit, wobei die Wahrscheinlichkeit der Gefahr eines 51%-Angriffs sehr gering ist.

Trotz der enormen Sicherheit der Blockchain lassen sich auf der technischen Seite bei der Nutzung dieser einigen Risiken, vor allem in der Usability und der Zugänglichkeit, identifizieren. Die größte Gefahr bei der unausgereiften Usability der Wallets liegt in der Möglichkeit des menschlichen Versagens. Fehlende Prüfmechanismen in Wallets können, ausgelöst durch einen Übertragungsfehler, zu einem Versenden des Betrages an eine falsche Adresse führen. Durch die Unumkehrbarkeit der Transaktionen besteht daher keine Möglichkeit die verlorene Summe zurückzuverlangen. Diese Risiken liegen dabei vor allem auf der Seite der privaten Nutzer, welche im Gegensatz zu

Unternehmen mit entsprechenden Schulungen, eine gewisse technische Affinität und Themenverständnis, sowie Einarbeitungszeit benötigen. Des Weiteren sind besonders Börsen als Sicherheitsrisiko einzustufen. Softwarewallets können dem Angriff von Hackern zum Opfer fallen, wohingegen Hardware- und Paperwallets zwar als sicher anzusehen sind, jedoch im Alltag, fern des Wohnraumes, aufgrund der Art der Nutzung nicht als praktikabel erachtet werden können. Wird ein Nutzer somit Opfer eines solchen Angriffs oder Betrugs, so haftet kein Intermediär für dessen Verlust. Als Schnittstelle für den Tausch von Bitcoin in andere Kryto-Währungen/ -Assets oder dessen Liquidierung stellen die unausgereiften und teilweise instabilen Krypto-Börsen ein Sicherheitsrisiko bei dem Erwerb oder dem Umtausch von Bitcoin dar.

Ein weiteres Risiko in der Nutzung Bitcoins als Zahlungsmittel lässt sich in der hohen Volatilität des Assets identifizieren. Diese verursacht mehrere Risiken, die sich in einer Hemmschwelle der Ausgabe von Bitcoins manifestieren. Zum einen verursacht die Volatilität eine damit einhergehende Preisschwankung, durch welche ein potenzieller Käufer eines Produkts dieses, zu unterschiedlichen Zeiten, zu unvorhersehbar unterschiedlichen Preisen erhält, wodurch eine Preisstabilität nicht gegeben ist. Zum anderen zeigt der volatile Kurs langfristig einen klaren Aufwärtstrend, welcher ein Halten von Bitcoins gegenüber einer Ausgabe dieser für viele attraktiver gestaltet. Im Vergleich zu einer stabilen, staatlichen Währung lassen sich auch hier keine Chancen in der Nutzung als Tausch- und Zahlungsmittel identifizieren. Des Weiteren gestaltet sich die Nutzung von Bitcoin aus der steuer- und finanzrechtlichen Perspektive weitaus aufwendiger als die Nutzung souveräner Währungen. Jegliche Wertsteigerung kann einen steuerrechtlichen Vorgang bedeuten. Tauscht ein Nutzer seinen Bitcoin nach Wertsteigerung in ein anderes Krypto-Asset oder eine Währung um, oder nutzt dies zur Bezahlung, so gilt es, diesen Wertgewinn zu versteuern und in den Aufzeichnungen für das Finanzamt zu erfassen. Auch erfordert die Nutzung eine gewisse Rücklage der landeseigenen Währung, um die Wertgewinne in dieser an das Finanzamt zu entrichten. Erfolgt dies nicht, ist ein, mit Gebühren verbundener, Umtausch der Einheiten in die Währung von Nöten, was wiederrum einen steuerrechtlichen Vorgang mit sich ziehen kann. Verglichen mit der Nutzung staatlicher Währungen lässt sich dementsprechend das Risiko eines großen bürokratischen Aufwands feststellen. Auch stellt die für die Unternehmen unvorteilhafte Rechtslage bezogen auf das Reklamationsrecht ein Risiko dar. Zusätzliche Risiken, verursacht durch eine unklare Rechtslage, lassen sich bei dem Thema Marktmanipulation identifizieren. Dieses Risiko nimmt jedoch mit zunehmender Marktkapitalisierung immer weiter ab. Rechtliche Chancen ergeben sich dabei nur durch die Transparenz der Blockchain.

Diese ermöglicht eine Rekonstruktion der Nachweise für Wertgewinne und/oder Wertverluste.

Die Zusammenfassung der zentralen Forschungsergebnisse zeigt auf, dass die vier aufgestellten Hypothesen verifiziert werden können. Bitcoins Systemarchitektur sowie dessen marktwirtschaftliche Einflüsse verhindern eine effiziente Nutzung dessen als Tausch-und Zahlungsmittel. Die Transaktionszeiten und vor allem -kosten machen eine Zahlung unwirtschaftlich, sowohl auf der Seite der Käufer, als auch auf Seiten der Verkäufer. Ferner sind diese Nachteile gegenüber den zentralen Zahlungsmitteln nicht ohne eine Nutzung von Drittanbietern, bei welchen es noch keine vollends entwickelte und getestete Lösung gibt, auszugleichen. Die Verifizierung dieser Hypothesen erlaubt somit ebenfalls eine Bestätigung der These, wodurch sich die Forschungsfrage wie folgt beantworten lässt: *Bitcoin bieten sich im aktuellen technischen Zustand geringe Chancen als Tausch-und Zahlungsmittel in der breiten Menge genutzt zu werden*. *Lediglich der Einsatz als Nischenalternative zu herkömmlichen Währungen bietet sich in wenigen Fällen an.*[61]

4. Fazit und Ausblick

Bitcoin wurde als Tausch- und Zahlungsmittel konzipiert und lässt sich auch als solches nutzen. Die Chancen und Risiken einer Nutzung, welche sich aus den systeminternen und -externen Einflüsse ergeben, wurden im Rahmen dieser Arbeit untersucht.

Die theoretische Auseinandersetzung mit dem zu bearbeitenden Bereich in der vorliegenden Disziplin ergab, dass Bitcoin als hybrides Krypto-Asset und nicht als Währung zu definieren ist. Weiterhin wurden durch die Analyse der Eigenschaften des Systems hohe Transaktionskosten und -zeiten im Vergleich zu herkömmlichen Zahlungsmitteln identifiziert. Die reine Preisbestimmung durch den Markt hat eine durchgehende Volatilität zur Folge, wohingegen zentral gesteuerte Währungen durch ihr Streben nach annähernder Preisniveaustabilität Vorteile in der Nutzung als Tausch- und Zahlungsmittel mit sich bringen. Festgestellt wurde weiterhin, dass der Bitcoin dennoch die erste dezentrale und Einheiten-endliche Alternative gegenüber diesen darstellt.

[61] Der Autor weist an dieser Stelle darauf hin, dass die Entwicklung bislang unbekannter Technologien nicht vorausgesagt werden kann, welche rein theoretisch in der Lage wären, Lösungen für identifizierte Risiken wie das Skalierungsproblem aufzuzeigen.

Die vorliegende Untersuchung kommt dementsprechend zu dem Ergebnis, dass eine Nutzung des Bitcoins als Tausch- und Zahlungsmittel lediglich Chancen in der Nutzung als dezentrale Alternative mit sich bringt, die identifizierten Risiken dieses Medium jedoch zum aktuellen Zeitpunkt nicht massentauglich machen und sich nur wenige Use-Cases mit Vorteilen gegenüber herkömmlichen staatlichen Zahlungsmitteln ermitteln lassen. Trotz der Verifizierung der anfangs aufgestellten (Hypo-) These(n) lassen sich für eine erweiterte Betrachtung des Gesamtbildes weiterführende Forschungsansätze erarbeiten. Im Folgenden werden dementsprechend Empfehlungen ausgesprochen.

Die Anwendung eines wissensaneignenden Forschungsdesigns in der Ausprägung von leitfadengestützten Experteninterviews und einer qualitativen Inhaltsanalyse brachte neue Erkenntnisse, sowie eine Absicherung der erarbeiten theoretischen Erkenntnisse, bezüglich der Chancen und Risiken von Bitcoin als Tausch- und Zahlungsmittel hervor. Daran anknüpfend bietet sich eine Erhebung quantitativer Daten durch ausgewählte quantitative Methoden mit dem Ziel an, das erlange Wissen zu erweitern und zu präzisieren. Eine Forschungsmöglichkeit lässt sich in der Frage identifizieren, wie groß der Bedarf der Zahlungsmöglichkeit mit Bitcoin zu begreifen ist.

Diese Arbeit behandelt die Chancen und Risiken eines bestimmten dezentralen Mediums in dessen aktuellem Zustand. Aus diesem Grund gilt es weiterführend qualitativ zu untersuchen, wie hoch der Nutzen eines dezentralen Systems generell sein kann. Eine Ökonomie mit einer endlichen Währung würde in einem deflationären Umfeld operieren. Aufgrund der dezentralen Eigenschaften gibt es für das System keine Möglichkeit das Verhältnis von Angebot und Nachfrage zu regulieren. Dies hat eine durchgehende Volatilität zur Folge, die mit der von Rohstoffen wie Gold verglichen werden kann. Charrier (2017) merkt in Zeile 332-333 an, dass die durchschnittliche Lebensdauer einer Währung bei 27 Jahren liegt, wobei der Wert jeden Systems bisher über Zeit auf null gegangen ist. Ramb (2017) betont des Weiteren, dass der Anreiz das Geld zu vermehren um das eigene Wirtschaftssystem oder sonstige Interessen zu unterstützen für jede herrschende Kraft zu groß ist (Z. 354). Im Zuge dessen lässt sich auch analysieren, wie hoch der Nutzen eines Systems sein kann, in welchem die Geldmenge kontrolliert und absehbar ist.

Weiterführend lässt sich eine Empfehlung hinsichtlich des Vergleichs mit spezifischen Währungssystemen jeweiliger Länder als möglichen Forschungsansatz aussprechen. Jedes Land auf der Welt befindet sich in unterschiedlichen wirtschaftlichen Situationen. In einigen Ländern kann es daher vorkommen, dass der Bitcoin weniger Volatilität

aufweist, als die nationale Währung selbst. In einem solchen Fall lassen sich ganz neue Einflüsse identifizieren, die es zu erforschen gilt. Damit einher geht auch die Nutzung von Bitcoin als Wertspeicher. Volatil, mit dennoch durchgehend ansteigender Tendenz des Wertes bieten die deflationären Eigenschaften eine Nutzung als Wertspeicher und/oder Spekulationsobjekt. Um weitere Aussagen über die daraus entstehenden Chancen und Risiken für Länder mit volatilen Währungen oder solcher mit stabilen zu treffen, bietet sich eine wissenschaftliche Forschung dementsprechend an.

Durch die Forschung in der Disziplin konnten relevante und neue Erkenntnisse hinsichtlich der Betrachtung Bitcoins in der Rolle als Tausch- und Zahlungsmittel gewonnen werden. Des Weiteren ermöglichte das Forschungsdesign eine Identifikation weiterer sozialer Probleme und ableitbarer Forschungsansätze, welche mit Hilfe weiterer qualitativer und/oder quantitativer Forschung angegangen werden können. Eine Auswahl der Experten aus verschiedenen Bereichen, welche die Berührungspunkte mit dem Thema vereint, erwies sich weiterhin als sehr wertvoll im Hinblick auf das gewonnene Spezialwissen. Trotz einer möglichen Kritik an der Datenerhebungsmethode *Experteninterviews*, bei welcher die Wahl einer geringen Stichprobe und die damit einhergehende Möglichkeit einer geringen Repräsentativität als problematisch erachtet werden kann, bietet sich dieser Kritik im Falle dieser Arbeit kein Halt. Ziel der vorliegenden Arbeit ist es eine komplexe, fremde Disziplin zu verstehen und ein bestimmtes Thema in dieser kritisch zu hinterfragen. Das leitfadengestützte Experteninterview stellt dabei die ideale Methode der Datenerhebung dar. In Anbetracht der genannten Punkte kann die Verwendung dieser Forschungsmethode demnach als angemessen betrachtet werden. Fundamental war auch die Bearbeitung der erhobenen Daten mittels der qualitativen Inhaltsanalyse und dem hierbei erstellten Kategoriensystem zum Zwecke der inhaltlichen Strukturierung der extrahierten Daten.
Dabei erwiesen sich sowohl die Transkriptionen der Experteninterviews, als auch die sorgfältige und detaillierte Durchführung der Analyse der sehr umfangreichen Datenmenge dem Autor gegenüber als eine partiell erwartete große Herausforderung, deren Bezwingung hohen zeitlichen Aufwand erforderte.
Ungeachtet dessen belohnte dieser Einsatz den Forschenden in der betrachteten Disziplin mit wertvollen Erkenntnissen und umfangreichem Wissen, wodurch sich der Abschluss des Studiums aus der Perspektive des Verfassers als gelungen erweist.

Quellenverzeichnis

Beitrag

Teo, E. (2018). Chapter 10 - Legal Risks of Owning Cryptocurrencies. In Academic Press (Ed.), Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1 (pp. 225–247). Academic Press. In https://doi.org/10.1016/B978-0-12-810441-5.00010-5

Buch (Monographie)

Achim Poller, Bernd Kirchner, & Polzin, J. M. (2010). Duden Wirtschaft von A bis Z: Grundlagenwissen für Schule und Studium, Beruf und Alltag (4. Aufl.). Mannheim: Dudenverl.

Bheemaiah, K. (2017). The Blockchain Alternative: Rethinking Macroeconomic Policy and Economic Theory. Berkeley, CA: Apress.

Bieder, J. (2012). Fremdwährungsrisiken im Außenhandel: Strategien und Instrumente zur Absicherung (1. Aufl.). s.l.: Diplomica Verlag GmbH.

Campbell-Verduyn, M. (2018). Bitcoin and beyond: Cryptocurrencies, blockchains and global governance. RIPE series in global political economy. Abingdon, Oxon, New York, NY: Routledge.

Cheung, H. (2017). Gold and international finance: The gold market under the internationalization of RMB in Hong Kong. Routledge advances in risk management: Vol. 8. London, New York: Routledge Taylor & Francis Group.

Colbe, W. B., & Laßmann, G. (1991). Betriebswirtschaftstheorie: Grundlagen, Produktions- und Kostentheorie (Fünfte, durchgesehene Auflage). Springer-Lehrbuch. Berlin, Heidelberg: Springer.

Dannen, C. (2017). Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. New York: Apress.

Davidson, J. D., & Rees-Mogg, W. (1997). The sovereign individual: Mastering the transition to the information age (1st ed.). New York, NY: Touchstone/Simon & Schuster.

Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. New York: Apress.

Evans, N. D. (2003). Business innovation and disruptive technology: Harnessing the power of breakthrough technology --for competitive advantage. Financial Times Prentice Hall books. Upper Saddle River, NJ: Financial Times Prentice Hall.

Gläser, J., & Laudel, G. (2009). Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen (3., überarb. Aufl.). Lehrbuch. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kaiser, R. (2014). Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung. Lehrbuch. Wiesbaden: Springer VS.

Karame, G. O., & Androulaki, E. (2016). Bitcoin and Blockchain Security. Norwood: Artech House.

Kippenhahn, R. (2012). Verschlüsselte Botschaften: Geheimschrift, Enigma und digitale Codes (Überarb. und erw. Neuausg). Rororo: Vol. 62761. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.

Laux, H. (2007). Entscheidungstheorie (7., überarb. und erw. Aufl.). Springer-Lehrbuch. Berlin: Springer.

Luhmann, N. (1997). Gesellschaft der Gesellschaft (1. Aufl.). Frankfurt am Main: Suhrkamp.

Mayring, P. (2016). Einführung in die qualitative Sozialforschung: Eine Anleitung zu qualitativem Denken (6., überarbeitete Auflage). Pädagogik. Weinheim, Basel: Beltz.

Morabito, V. (2017). Business Innovation Through Blockchain: The B³ Perspective. Cham: Springer International Publishing.

Mullan, P. C. (2016). A History of Digital Currency in the United States: New Technology in an Unregulated Market. Palgrave Advances in the Economics of Innovation and Technology. New York: Palgrave Macmillan US.

O'Sullivan, A., & Sheffrin, S. M. (2004). Economics: Principles in action. Princeton, N.J.: Recording for the Blind & Dyslexic.

R. C. Merkle. (1988). Advances in cryptology - CRYPTO '87: Lecture Notes in Computer Science. Advances in cryptology: Vol. 7.1987. Berlin: Springer.

Raval, S. (2016). Decentralized applications: Harnessing Bitcoin's Blockchain technology (First edition). Sebastopol, CA: O'Reilly Media.

Singh, S. (2001). Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet ([Nachdr.]). München: Hanser.

Sixt, E. (2017). Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie. Wiesbaden: Springer Gabler.

Stocker, K. (2006). Management Internationaler Finanz- und Währungsrisiken (2., vollständig überarbeitete Auflage). Wiesbaden: Betriebwirtschaftlicher Verlag Dr. Th. Gabler | GWV Fachverlage GmbH Waisbaden.

Swan, M. (2015). Blockchain: Blueprint for a new economy (1. ed.). Safari Tech Books Online. Beijing: O'Reilly.

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business and the world. New York, New York: Portfolio/Penguin.

Tapscott, D., & Tapscott, A. (2016). Die Blockchain-Revolution: Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert (2. Auflage). Kulmbach: Plassen Verlag.

Weltwirtschaftsforum; Deloitte. (2016). The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services : an industry project of the financial services community : part of the future of financial services series. Future of financial services series. Cologny/Geneva: World Economic Forum.

Wildmann, & Lothar. (2007). Module der Volkswirtschaftslehre. Module der Volkswirtschaftslehre: Vol. 02. München, Wien: Oldenbourg.

Wildmann, L. (2010). Makroökonomie, Geld und Währung: Module der Volkswirtschaftslehre Band II (2., überarb. und verb. Aufl.). VWL, 10-2012. München: Oldenbourg.

Buch (Sammelwerk)

Academic Press (Ed.). (2018). Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Academic Press.

Dinel Wilusz (Ed.). (2011). Macro determinants of operation of e-money systems in European Union. Sopot, Gdańsk: Department of Information Technology.

ETLA Elinkeinoelämän Tutkimuslaitos - The Research Institute of he Finnish Economy (Ed.). (2017). Smart Contracts – How will Blockchain Technology Affect Contractual Practices? (1st ed., Vol. 68).

Fritz Knapp Verlag (Ed.). (2017). Blockchain: Mehr als ein Hype? Zeitschrift für das gesamte Kreditwesen: Vol. 11. Frankfurt am Main: Fritz Knapp Verlag.

Ledger: The journal of cryptocurrency and blockchain technology research. (2016). Pittsburgh, PA: University Library System University of Pittsburgh.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton: Princeton University Press.

N.A. (2018). Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1. Academic Press.

Springer Gabler (Ed.). Business & information systems engineering : BISE : the international journal of Wirtschaftsinformatik.

Graue Literatur / Bericht / Report

Board of Governors of the Federal Reserve System. (1963). Guide to Legislative History of the Original Federal Reserve Act. Retrieved from Federal Reserve Bank website: http://www.llsdc.org/assets/FRAdocs/fra-guide-leg-hist.pdf

Internetdokument

Börsenlexikon. (2017). Milchmädchen Hausse. Retrieved from http://www.boersennews.de/lexikon/begriff/milchmaedchen-hausse/1826

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). (2014). Aufgaben & Geschichte der BaFin. Retrieved from Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Coingecko. (2017). Bitcoin Kurschart 18.12.2017 00:00 Uhr. Retrieved from https://www.coingecko.com/de/kurs_chart/bitcoin/btc

Jonas Chokun. (2018). Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops. Retrieved from https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

Satoshi Nakamoto. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Xe Währungsrechner. Bitcoin to USD. Retrieved from http://www.xe.com/de/currencyconverter/convert/?Amount=1&From=XBT&To=USD

Pressemitteilung

Bloomberg L.P. (2017). Internet Software and Services: Company Overview of Coinbase, Inc. Retrieved from https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=225488472

Deutsche Börse. (2016). Deutsche Börse startet neuen XDAXDAX-Index: Index deckt gesamte Handelszeit des Derivatemarktes ab. Retrieved from http://deutsche-boerse.com/dbg-de/presse/pressemitteilungen/Deutsche-Boerse-startet-neuen-XDAXDAX-Index/2386400

DailyTech. (2011). Inside the mega hack of Bitcoin: The full story. Retrieved from https://web.archive.org/web/20140210122955/https://www.mtgox.com/press_release_20140210.html

Mt. Gox. (2017). Pressrelease 10.02.2017. Retrieved from https://web.archive.org/web/20140210122955/https://www.mtgox.com/press_release_20140210.html

Valve Corporation. (2017). Bitcoin wird auf Steam nicht mehr unterstützt. Retrieved from https://steamcommunity.com/games/593110/announcements/detail/1464096684955433613

Unklarer Dokumententyp

Bank für Internationalen Zahlungsausgleich. 83. Jahresbericht, pp. 5–9. Retrieved from https://www.bis.org/publ/arpdf/ar2013_de.pdf

Catalin Cimpanu. (2018). Microsoft Halts Bitcoin Transactions Because It's An "Unstable Currency". Retrieved from https://www.bleepingcomputer.com/news/cryptocurrency/microsoft-halts-bitcoin-transactions-because-its-an-unstable-currency-/

Zeitschriftenaufsatz

Bakshi, G., & Panayotov, G. (2013). Predictability of currency carry trades and asset pricing implications. Journal of Financial Economics. (110), 139–163. https://doi.org/10.1016/j.jfineco.2013.04.010

Cooper, R. V. L. (1974). Efficient Capital Markets and the Quantity Theory of Money. The Journal of Finance, 29(3), 887–908. https://doi.org/10.1111/j.1540-6261.1974.tb01489.x

European Central Bank. (2004-2008). The implementation of monetary policy in the euro area: The implementation of monetary policy in the euro General documentation on eurosystem monetary policy instruments and procedures. (83), 1–122.

Fand, D. I. (1970). A Monetarist Model of the Monetarist. The Journal of Finance, 25(2), 275–289. https://doi.org/10.1111/j.1540-6261.1970.tb00506.x

Gürcan Öndner, Antonella Del Pozzo, & Sara Tucci-Piergiovanni. (2017). On the Bitcoin Limitations to Deliver Fairness to Users. International Conference on Cooperative Information Systems. (25).

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. Telematics and Informatics, 2017(34), 1308–1321. https://doi.org/10.1016/j.tele.2016.05.005

Jakub W. Jurek. (2014). Crash-neutral currency carry trades. Journal of Financial Economics. (113), 325–347.

Juri Mattila. (2016). The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures. ETLA Working Papers. (38). Retrieved from https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdf

Kerry Lynn Macintosh. (1998). How to encourage global electronic commerce: The case for private currencies on the internet. Harvard Journal of Law & Technology, 1988(3), 739–796.

Kessel, R. A., & Alchian, A. A. (1962). Effects of Inflation. Journal of Political Economy, 70(6), 521–537. https://doi.org/10.1086/258714

Kiyotaki, N., & Wright, R. (1989). On Money as a Medium of Exchange. Journal of Political Economy, 97(4), 927–954. https://doi.org/10.1086/261634

Klopstock, F. H. (1965). The International Money Market: Structure, Scope and Instruments. The Journal of Finance, 20(2), 182–208. https://doi.org/10.1111/j.1540-6261.1965.tb00203.x

Marc-David L. Seidel. (2017). Questioning Centralized Organizations in a Time of Distributed Trust. Journal of Management Inquiry, 1–5.

Nicholas Plassaras. (2013). Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. Chicago Journal of International Law, 1–26.

Niklas Luhmann. (1984). Die Wirtschaft der Gesellschaft als autopoietisches System. Zeitschrift für Soziologie, 13(4).

R.C. Merkle. Protocols for public key cryptosystems. IEEE Computer Society, 1980, 122–133.

Tom Simonite. (2014). The Man Who Really Built Bitcoin. MIT Technology Review. Retrieved from https://www.technologyreview.com/s/527051/the-man-who-really-built-bitcoin/

W. Diffie, & M. Hellman. (1976). New directions in cryptography. Institute of Electrical and Electronics Engineers (IEEE), 1976(22), 644–654. Retrieved from New directions in cryptography

Wallace, N. (2014). Optimal money creation in “pure currency” economies: A conjecture The Quarterly Journal of Economics, 129(1), 259–274. https://doi.org/10.1093/qje/qjt030

Zeitungsartikel

Reuters Redaktion (2017, December 12). BÖRSEN-TICKER-Erneuter Hacker-Angriff auf Bitcoin-Börse Bitfinex. Reuters, pp. 1–4. Retrieved from https://de.reuters.com/article/mrkte-idDEL8N1OC5FP

Anhang

Anhang 1: Interviewleitfaden

1. Anfangs möchte Ich Sie einmal bitten, Ihren Werdegang, Ihre derzeitige Tätigkeit, sowie Ihre Berührungspunkte mit dem Thema kurz zu beschreiben

2. Als welche Art von Medium ist Bitcoin zu definieren?

3. Als wie effizient ist die System-Architektur der Blockchain zu betrachten?

4. Welche Chancen und Risiken lassen sich in dieser im Hinblick auf eine Nutzung als Tausch-und Zahlungsmittel identifizieren?

5. Kann die Nutzung Bitcoins ökonomisch effizient gestaltet werden?

6. Welche Probleme ergeben sich durch die Volatilität des Bitcoins?

7. Als wie sicher ist die Nutzung der Blockchain zu erachten?

8. Wie einfach gestaltet sich die Durchführung einer Transaktion?

9. Entstehen Risiken durch die Zentralisierung der Miningpools?

10. Welche finanz- und steuerrechtlichen Rahmenbedingungen herrschen bei der Nutzung von Bitcoin als Tausch- und Zahlungsmittel für private/juristische Personen?

11. Gibt es fragile Knoten im Blockchan-Netzwerk?

12. Welche Risiken und/oder Chancen ergeben sich durch den elitären Kreis der Entwickler und Nodebetreiber?

Vielen Dank, dass Sie sich die Zeit genommen haben mit mir über die Chancen und Risiken von Bitcoin als Krypto-Asset zu sprechen!

Anhang 2: Ergebnisübersicht: Qualitative Inhaltsanalyse

Forschungsfrage	Welche Chancen und Risiken ergeben sich der Nutzung von Bitcoin als Tausch-und Zahlungsmittel?					
Beschreibung	Mittels der angewandten Forschungsmethoden soll herausgefunden, welche inneren und äußeren Faktoren auf das Medium einwirken und die Chancen, sowie Risiken erschaffen.					
Art der Inhaltsanalyse	Deduktiv - Inhaltliche Strukturierung					
Bewertung	Übereinstimmend	Ähnlich	Unterschiedlich	Keine Angaben		
Experten	Technische Effizienz	Ökonomische Effizienz	Technische Sicherheit und Usability	Gesetzliche Regelungen	Stabilität des Ökosystems	Definition Bitcoins
Patrick Charrier	Die Transaktionszeiten sind im Vergleich zu herkömmlichen Zahlungsmitteln sehr lang. Vorteil gegenüber internationalen Transaktionen. Betrug durch Irreversibilität nicht möglich.	Hohe Transaktionskosten machen Bitcoin im nationalen Raum und bei Transaktionen in geringer Höhe nicht ökonomisch. Im internationalen Raum kann es jedoch zu Zeitersparnissen kommen, welche einem Unternehmen ökonomisch von Vorteil sein können. PayPal und Visa etc. sind dem medium jedoch voraus. Auch die Volatilität stellt ein großes Problem dar.	Die Nutzung erweist sich als kompliziert und die Nutzer müssen die technischen Grundlagen verstanden haben, um sich sicher im Ökosystem zu bewegen. Hierbei ist ein Lernprozess von Nöten. Die Blockchain ist allerdings als sehr sicher einzustufen.	Der Versteuerung der Gewinne wird nach und nach mehr nachgegangen werden. Viele Staaten werden noch weitere Maßnahmen ergreifen, ein Bekämpfen des Ökosystems würde jedoch nur in wirtschaftlichem Nachteil für diesen enden.	Der Kreis, der sich um die Weiterentwicklung von Bitcoin kümmert und die wichtigen Entscheidungen trifft, ist sehr klein und elitär. Dennoch hat dieser ein großes Interesse an dem Fortbestand und dem Gedeihen des Systems, wodurch Stabilität gewährleistet wird.	Nur bedingt als Währung einzustufen.
Christopher Nigischer	Nur gegenüber Internationalen Überweisungen geschwindigkeitstechnisch überlegen. Herkömmliche Zahlungsanbieter werden immer effizienter und entwickeln ihre Technologie weiter.	Die hohen Transaktionsgebühren machen Bitcoin unwirtschaftlich. Auch die Volatilität stellt sich einer effizienten Nutzung als Zahlungsmittel gegenüber. Eine stabile Wirtschaftlichkeit ist vorerst nicht gegeben.	Abgesehen von der Usability ist das System als sehr sicher einzustufen. Die Gefahr des Vertippens stellt jedoch ein großes Risiko dar. Die Möglichkeit eines menschlichen Fehlers wird in dem aktuellen System nur geringfügig minimiert.	Es kann zum Konflikt mit der Datenschutzgrundverodnung kommen, da der Umgang mit Geld privat bleiben sollte. Sich als Nutzer auch hier in diesem Raum Anonym zu bewegen ist möglich, aktuell jedoch schwer umzusetzen und nicht auf die breite Masse ausgelegt. Eine Nutzung wird Lernprozesse erfordern. Aktueller gesetzlicher Rahmen reicht aus und muss nur auf Bitcoin bezogen werden.	Durch die hohe Marktkapitlisierung senkt sich die Volatilität fortlaufend und die Stabilität nimmt zu. Alle incentivierten Teilnehmer des Ökosystems haben ein Interesse am sicheren Bestand Bitcoins. Dennoch ist die Gruppe, die über diesen Fortbestand wacht in gewissen Maße sehr klein. Stabilität ist also vorhanden, Fragilität jedoch nicht auszuschließen.	Aktuell eher für Use-Cases wie Wertspeicherung oder Trading-Objekt geeignet.

Florian Fiedler	Eleminierung von Intermediären theoretisch effizient, praktisch steht es jedoch noch vor großen Herausforderungen.	Als Tausch-und Zahlungsmittel ist Bitcoin nicht ansatzweise so effizient wie das VISA-Netzwerk. Dabei sind andere Kryptowährungen kosten- und zeiteffizienter. Bitcoin wird sich als Währung nicht gegen Fiat-Geld behaupten können. Beim Kauf mit Bitcoin stellt die Volatilität dabei eine große Hürde dar.	Die Blockchain an sich ist extrem sicher. Die zur Anwendung benötigte Technologie ist dagegen in der Nutzung noch etwas unausgereift. Schulungen können in Unternehmen von Nöten sein. Für Privatanwender besteht eine größere Hürde.	Durch die Blockchain ist es einfacher den eigenen Zahlungsverkehr zu rekonstruieren. Eine Bezahlung über Bitcoin anzunehmen ist für den Steuerberater ein Alptraum. Zum Thema Marktmanilation sind noch einige Gesetze zu erwarten.	Trotz der fortschreitenden Zentralisierung der Miner ist das System als stabil einzustufen. Marktmanipulation ist jedoch ein Problem.	Nicht als Währung einzustufen
Benjamin Kirschbaum	Die mathematischen und kryptographischen Eigenschaften machen das System effizient in der Sicherheit der Blockchain, der Open-Source Code das Netzwerk transaparent.	Die Volatilität nach oben stellt eine große Hemmschwelle für das Ausgeben von Bitcoins dar. Die Besteuerung führt zu einem enormen buchhalterischen Aufwand, sowie zu Umkosten.	Die Nutzung ist, für jemanden der sich etwas auskennt, sehr sicher. Bitcoin ist dabei, als bewährtes System enorm sicher. Das System ist allerdings noch anfällig für viele menschliche Fehler.	Steuerrechtlich muss darauf geachtet werden, eventuelle Wertsteigerungen zu versteuern. Viele bestehende Gesetze in Deutschland greifen dabei auf Bitcoin über. Börsen gelten als Finanzdienstleistungsunternehmen und werden durch die BaFin geregelt.	Hardforks und Hacks haben das System gestärkt anstatt es zu schwächen. Durch die alleinige Regelung des Marktes ist Bitcoin sehr sicher, da das Wertversprechen durch das System und seine Nutzer selbst entsteht, die alle ein Interesse an dessen Fortbestand haben. Zentralbanken stellen Gefahren für die Stabilität der Währungen dar.	Nur bedingt als Währung einzustufen.
Daniel Jeffries	Machtverteilung funktioniert demokratisch und Peer-to-Peer. Kleiner Kreis bestimmt über die technische Zukunft des Mediums.	Ökonomisch betrachtet ist das System nicht als effizient zu betrachten. Die Volatilität wird noch einige Jahre anhalten und sich dann langsam senken. Kurzfristig betrachtet wird es profitabler sein Bitcoin zu halten, statt sie auszugeben.	Werden die Core-Wallets genutzt, so kann Bitcoin als sehr sicher eingestuft werden. Durch das Lightning-Network wird das Skalierungsproblem gelöst werden. Aktuell kann die Usability nicht als gut eingestuft werden.	-	Der Markt selbst hat ein Interesse daran, das Ökosystem aufrecht zu erhalten. Bitcoin eröffnet durch die Blockchain erstmalig harte Versprechen. Marktmanipulation stellt ein großes Manko dar, kann aber bei Größerwerden der Währung einfach bekämpft werden.	Bitcoin ist eher als Wertspeicherungsmittel anzusehen. Seine Eigenschaften erlauben auch Zahlungen, eignen sich aber weitaus weniger als herkömmliche Mittel und Kryptowährungen. Bitcoin ist nicht als klassische Währung, sondern as hybrides Asset zu definieren.
Darshini Dalal	Bitcoin bietet viele Vorteile gegenüber dem traditionellen Bankensystem. Der Nutzer verfügt selbst über seine Werte und benötigt keine Intermediäre.	Bitcoin ist nicht ökonomisch und sollte auch nicht als Zahlungsmittel eingeführt werden. In den kommenden Jahren kann dies durch technologische Meilensteine gelöst werden.	Wenn sich der Nutzer vorsichtig verhält besteht keine Gefahr und Sicherheit ist garantiert. Die Nutzer müssen allerdings über eine korrekte Nutzung aufgeklärt werden. Ein weiteres Problem stellt das Fehlen von Governance dar.	-	Die Stabilität hängt stark von einer kleinen Gruppe ab. Dennoch hat sich Bitcoin bisher als enorm stabil erwiesen, was daraufhin weist, dass der Markt ein großes Interesse an der Stabliität hat. Forks bieten hierbei mehr oder weniger demokratische Optionen.	Nicht als Währung einzustufen.

Daniel Heller	Anonymität und Peer-to-Peer Eigenschaften bieten dem System alternative Chancen. Technische Vorteile gegenüber herkömmlichen Systemen bestehen jedoch nicht. Die Zeit bis zur Irreversibilität dauert zu lange und ist bei Handelspartnern mit hohen Beträgen nicht erwünscht.	Alle Studien zeigen, dass Bitcoin nur sehr wenig als Zahlungsmittel verwendet werden und alle Besitzer diese, in Hoffnung auf Wertsteigerung, halten. Bitoin besitzt in der Geschwindigkeit und Kosten keine Vorteile gegenüber aktuellen Retail-Payment Systemen. Eine Off-Chain Lösung könnte Bitcoin wirtschaftlicher machen, wäre jedoch zentralisiert.	Die Blockchain ist als sehr sicher einzustufen. Vor allem aber die Exchanges nicht. Im Gegensatz zu herkömmlichen Handelsplattformen weisen diese enorme Defizite auf. Die Interaktion mit der Blockchain ist noch sehr hakelig. Aus lange Sicht kann dies jedoch gelöst werden.	Der Staat muss einen Weg finden, Guthaben korrekt zu besteuern. Regeln sind vorhanden, müssen jedoch noch durchgesetzt werden.	Forks sind eine gute Möglichkeit das System demokratisch zu stärken. Das Ökosystem an sich ist sehr stabil und gefährdet, im Falle eines Crashes, auch nicht das Fiat-Geld System.	Es wurde von einem Tauschmittel zu einem Spekualationsobjekt mutiert und weist daher Asset-ähnliche Schwankungen auf, die im Vergleich zu souveränen Währungen eine enorme ökonomische Hürde darstellen. Ist jedoch nicht eindeutig als Währung zu definieren.
Prof. Dr. Bernd-Thomas Ramb	-	Das Prinzip der Deflation hat den Nachteil, dass eine Hemmschwelle bei der Ausgabe der Bitcoin besteht. Vergleichbar mit dem Bankensystem der Zentralbanken werden sich weitere Subsysteme bilden, die als dritte Partei die Probleme der Dauer und der Kosten der Transaktionen Bitcoins mindern werden. Die ökonomischen Nachteile werden durch die hohe Nachfrage von Subsystemen des Marktes aufgefangen.	Die Eingabe einer falschen Adresse kann fatale Folgen haben. Eine Verbesserung der Usability ist exponentiell gebunden and die Zunahme der Attraktivität des Bitcoins. Die Massentauglichkeit nimmt also zu, je attraktiver Bitcoin von seinem Umfeld wahrgenommen wird.	Steuerrechtlich kommen viele bürokratische Schritte auf die Nutzer von Bitcoins, insbesondere in Unternehmen zu. Starke Eingriffe wie ein Verbot von Bitcoin ergeben auf staatlicher Seite keinen Sinn und wären auch nicht durchsetzbar.	Das Ökosystem hat sich trotz diverser Hacks und Probleme bisher als sehr stabil erwiesen. Der Dollar hat die gleiche Entwicklung durchgemacht. Der Vergleich der Stabilität muss immer mit dem jeweiligen Staat verglichen werden. Die Chancen und Risiken sollten immer mit denen der jeweiligen Währung verglichen werden.	Bitcoin ist jedoch definitorisch nicht als Währung einzustufen, wohingegen auch aktuelle souveräne Währungen die Kriterien nicht erreichen.

Anhang 3: Experteninterview Christopher Nigischer

Name	Christopher Nigischer
Aktuelle Institution	Chainstep GmbH / Innovationsforum Blockchain / NXP Semiconductors Germany
Funktionsbezeichnung/Titel	Geschäftsführer / u.a. Initiator / Projektmanager
Kontaktdaten	Griegstraße 75 22763 Hamburg 040 228678920 nigischer@consider-it.de
Datum des Interviews	30.11.2017
Freigabe	nicht erforderlich

I: Vielen Dank für Ihre Zeit. Vorab möchte ich Sie einmal bitten, sich ganz kurz vorzustellen mit Ihrem Werdegang, damit ich Sie in meiner Bachelorarbeit gut einordnen kann. #00:04:15-4#

Nigischer: Ich bin 38 Jahre alt, komme ursprünglich aus Österreich und bin seit 2005 in Hamburg. Ich habe in Österreich Betriebswirtschaftslehre berufsbegleitend studiert, habe in IT-Unternehmen vor allem auf der vertrieblichen Seite gearbeitet... hab hier in Hamburg dann bei der Technologieberatung einige Jahre eine Business-Unit aufgebaut und geführt und bin seit 2010 mit verschiedenen Firmen selbstständig, unter anderem mit der *consider it GmbH*, das war die erste Gründung, die IT-Consulting und Personaldienstleistungen erbringt und eine der jüngsten... oder die zwei jüngsten, die Blockchainbezug hat sind die *Chainstep GmbH*, die Blockchain vor allem im Bereich Supplychain-Management und Logistik in Projekten mit Kunden umsetzt und zum anderen mit *Asikos*, mit der wir, unter anderem, an der Entwicklung einer Token-Plattform, sowie am Thema ICO-Advisory arbeiten. #00:00:44-3#

I: Danke... alles klar. Dann würde ich gerne mit der zweiten Frage weitermachen – einer einfachen einleitenden Frage, mit wir besser auf die anderen eingehen können. Ich möchte Sie kurz bitte, die zentralen Eigenschaften einer Blockchain zusammenzufassen. #00:00:57-6#

Nigischer: Die Idee die dazu geführt hat, oder was man gesucht hat, ist Geld ohne Banken und eine Lösung für das Double-Spend Problem, dass man dann 2008 in dem

Whitepaper von Satoshi dokumentiert hat. Die damit verbundenen Eigenschaften sind Peer-to-Peer Kommunikation, Konsensprotokoll, Utibility und die Möglichkeit Werte oder Intermediäre auszutauschen, in digitaler Form. #00:01:32-1#

I: Vielen Dank, dann würde ich auch gleich auf die Nutzung von Bitcoin ein. Abgesehen von der Blockchain, als wie sicher erachten Sie Bitcoin bei der Nutzung von Wallets... Hard-Wallets oder Software-Wallets. Wie schätzen Sie das ein? #00:01:47-3#

Nigischer: Wie sicher das ist? #00:01:52#

I: Genau. Bei Ethereum gab es letztens ja zum Beispiel den Parity Bug, bei dem jemand 150 Millionen eingefroren hat. Als wie sicher sehen Sie das bei Bitcoin an? #00:02:01-7#

Nigischer: Ja, ich glaube die Sicherheit hat Ihre Schwächen, vor allem, wenn man es gemeinsam mit der Usability betrachtet. Grundsätzlich halte ich es schon für ziemlich sicher, aber wenn man selbst dann die Erfahrung macht, dass man Bitcoin an andere Adressen überweist und sich möglicherweise vertippt und dass da keine großartigen Prüfmechanismen dahinterstehen, ob das die gewünschte Adresse ist und keine Möglichkeit besteht, das Geld, bzw. die Coins zurückzuholen, da sind schon Risiken mit verbunden, die ich jetzt nicht unbedingt einem Mangel an Sicherheit zuschreiben würde, sondern es ist einfach ein systemimmanent und erfordert einfach eine andere Handhabe oder eine sehr große Sorgfalt der Nutzer. Je größer die Nutzerschaft wird, desto problematischer wird diese, und gleichzeitig haben wir die Übergänge hinein in die Bitcoin Blockchain, was wir hier ja auch angesprochen haben mit Wallets verschiedener Art. Dort bestehen natürlich Sicherheitsrisiken, was die Qualität der Implementierung anbelangt. #00:03:12-2#

I: Alles klar, vielen Dank. Damit wären wir auch quasi schon bei der nächsten Frage, dass Zahlungen nicht rückgängig gemacht werden können. Abgesehen von der angesprochenen Nutzung, sehen Sie noch weitere Vor- und/oder Nachteile für Unternehmen oder Endkunden? #00:03:22-5#

Nigischer: Also ich sehe es eigentlich eher als Vorteil, weil eine Handlung nicht einfach so zurückgeschraubt werden kann, ohne... dass man sich verständigt. Aber es erfordert halt von den Prozessen drum herum, die man sich gibt, beispielsweise so S-

Cross Services oder Ähnliches. Sowas erfordert mehr an Nachdenken als das, in den uns gewohnten, Zahlungssystemen wie PayPal oder VISA. #00:03:54-9#

I: Ok, dann würde ich noch auf einen technischen Aspekt eingehen. Aktuell sind die Transaktionszeiten, also die *Fees* ja relativ hoch. Je geringer man die Gebühren setzt, desto höher die Wartezeit... wenn man es denn im Wallet einstellen kann, bei vielen geht das ja nicht. Sehen Sie das Lightning-Network als einzige Möglichkeit für Bitcoin zu konkurrieren, oder wie schätzen Sie das ein? #00:04:17-1#

Nigischer: Ich fand es schade und überraschend, dass Segwit2x nicht kam. Wenn man jetzt auf den Kurs guckt, dann muss man sage: „Ja, das hat dem Netzwerk nicht unbedingt geschadet." Die Transaktionsgebühren in der aktuellen Höhe (Anmerkung des Autors: Stand 01.12.2017) verhindern Anwendungszwecke, die vor allem in Richtung Zahlung gehen und das ist auf jeden Fall ein Nachteil. #00:04:41-1#

I: Ok, alles klar. Dann gehen wir auch direkt zur nächsten Frage. Bitcoin ist ja relativ... oder komplett transparent. Man kann ja alle Zahlungen usw. nachvollziehen. Sehen Sie das Vor- und Nachteile? #00:04:54-4#

Nigischer: Das würde ich eher als Nachteil sehen. Umgang mit Geld, im privaten Sinne eher personenbezogenes Datum, das heißt, wir haben dort alleine schon mit dem Thema *Datenschutzgrundverordnung* einen Konflikt und Möglichkeiten Zahlungen privat auszuführen, die gibt es ja in technischer Hinsicht schon, das ist ja nicht unmöglich, aber aktuell in der technischen Implementierung nicht breit verfügbar. Da muss nachgebessert werden. #00:05:28-5#

I: Sehen Sie die Nachvollziehbarkeit auch als abschreckend für Unternehmen an? #00:05:32-7#

Nigischer: Ja, auf jeden Fall. #00:05:35-4#

I: Alles klar. Dann hätte ich noch eine Frage zur Fragilität des Systems. Bitcoin hängt ja von den Nodes, den Minern und den Entwicklern ab. Bei der letzten Hardfork (Anmerkung des Autors: Bitcoin Cash) kam es auch zu politischen Auseinandersetzungen. Als wie stabil schätzen Sie das Bitcoin System ein? #00:05:56-5#

Nigischer: Also... da ja hier schon einiges auf dem Spiel steht, und die... das ist echt eine gute Frage. Wie stabil schätzt man das ein? Im Augenblick habe ich das Gefühl, dass die Interessen zwar nicht immer auf einem Nenner sind, sondern zumindest soweit alle incentiviert sind, dass alle an einem sicheren Bestand von Bitcoin Interesse haben und da auch einen persönlichen Vorteil draus ziehen. Das gibt ein gewisses Maß an Stabilität, aber die Gruppe, die darüber wacht und vielleicht auch ein Stück weit herrscht... die ist schon echt klein. Das ist auf jeden Fall problematisch und eine kleine Gruppe heißt: Fragilität ist durchaus auch vorhanden. #00:06:48-2#

I: Ok, meine nächste Frage dreht sich um die Außenstehenden. Wenn ich jetzt als neuer Nutzer in Bitcoin einsteigen möchte und ich finde heraus, dass es, durch Hardforks entstandene, wobei ich auch nicht weiß was bedeutet, Versionen von Bitcoin gibt, wirkt das abschreckend? #00:07:01-9#

Nigischer: Auf den ersten Blick vielleicht. Aber wenn ich mir jetzt die Entwicklung von Bitcoin und Bitcoin Cash angucke und den Profit, den da viele draus gezogen haben, dann kann das auch positive Seiten haben, die im Augenblick eher überwiegen. #00:07:17-1#

I: Ok und sehen Sie auch in Problem mit dem immer zentralisierteren Proof-of-Work System? Würde da vielleicht Proof-of-Stake Vorteile bieten? #00:07:26-4#

Nigischer: Ich bin gespannt wie sich das Experiment bei Ethereum bewährt und gerade auch in Hinblick auf den Energie- und Umweltaspekt ist ein ewiges „Weiter so“ mit dem Mining wahrscheinlich nicht der richtige Weg. #00:07:46-7#

I: Alles klar. Ich bin bei meiner Recherche auch, wie im Leitfragebogen dargelegt, auf die Eigenschaften einer Währung gestoßen. Tausch- und Zahlungsmittel, Recheneinheit und Wertspeicherung. Sehen Sie das bei Bitcoin als gegeben? #00:08:04-1#

Nigischer: Durch die Transaktionskosten ist sicher das Thema Tausch- und Zahlungsmittel eingeschränkt. Ebenso das Thema Recheneinheit, weil es durch die hohe Volatilität keine hinreichende Stabilität gibt... was natürlich auch gegeben ist, aber auch unter der Volatilität leidet, aber tendenziell kennt ja der Kurs seit über einem Jahr primär eine Richtung, nämlich die nach oben, sodass das Thema Wertspeicherung, vor allem im Vergleich mit so manchen Fiat-Währungen mit sehr hoher Inflation auf jeden Fall gegeben ist. #00:08:46-3#

I: Würden Sie Bitcoin eher als Spekulationsobjekt oder als Medium of Exchange, als als Tausch- und Zahlungsmittel einstufen? #00:08:54-1#

Nigischer: Primär... also ich sehe es nicht als Tausch-und Zahlungsmittel, dafür sind wie gesagt die Transaktionskosten zu hoch im Augenblick. Ich sehe es aber nicht nur als reines Spekulationsinstrument, sondern... wie gesagt, Menschen in Venezuela, für die das einfach eine Möglichkeit ist, sich vor der Inflation zu retten, da ist Spekulation nicht der primäre Zweck, sondern es ist eben die Wertspeicherung. #00:09:25-1#

I: Und würden Sie Bitcoin dabei als den idealen Platz sehen (Anmerkung des Autors: ideales Asset), oder versprechen Altcoins dabei mehr? #00:09:36-1#

Nigischer: Es ist die am breitesten akzeptierte denke ich, und auch wenn wir jetzt jenseits der 200 Milliarden Marke Kapitalisierung aller Krypto-Währungen reden, dann ist das immer noch nicht viel Geld und keine große Substanz. Je mehr sich das diversifiziert und sich die Marktkapitalisierung auf viele Währungen verteilt, desto weniger Liquidität und umso mehr Probleme mit Volatilität habe ich in den einzelnen Währungen. Insofern halte ich eine Fokussierung auf Bitcoin nicht für schlecht. #00:10:09-5#

I: Ok, ich hätte noch eine weitere Frage zu Stabilität. Durch die Dezentralität beruht Bitcoin ja einzig auf dem Vertrauen der Nutzer in das System selbst. Es gibt keine zentrale Entität wie die EZB oder die IMF, die dort Stabilität gewährleistet. Wie ordnen Sie das ein? #00:10:27-8#

Nigischer: Ja, es ist ein großes Experiment mit mittlerweile echt viel Geld. Ich sehe da die Chance, dass wir als Gesellschaft etwas lernen können, nämlich, dass es auch ohne eine zentrale Instanz funktionieren kann und das gut designte Systeme hier... teure Organisationen auch ersetzen können. Also primär eine Chance. #00:10:55-5#

I: Dann würde ich noch einmal auf die Volatilität zu sprechen kommen. Welchen Einfluss hat das auf Bitcoin als Handelswährung, wenn Amazon und Microsoft und weitere große Firmen Bitcoins zu akzeptieren? Ist es überhaupt wirtschaftlich Bitcoins zu nutzen, wenn der Nutzer sich sagt: „Oh, es könnte auch morgen schon weitaus mehr wert sein. Will ich das überhaupt ausgeben?“ #00:11:15-6#

Nigischer: [lacht] Ja, es kann wirtschaftlich sein, ist nur mit einem hohen Risiko im Moment verbunden. Ich glaube für... über den Erprobungsfall hinaus, nehme ich das wahr, dass man damit momentan einfach herumexperimentiert und ausprobiert wie das funktioniert. Solche Lösungen sind ja dann auch schon vorhanden, die dann Menschen vornehmen und eine Stabilität hereinbringen und trotzdem die Flexibilität der Kryptowährungen (Anmerkung des Autors: mit sich bringen. Solche Mittel muss man dann zusätzlich heranbringen. Aber aktuell sehe ich es primär als laufendes Experiment. #00:11:58-1#

I: Ok, dann hätte ich noch eine tiefgehende Frage. Das ist jetzt natürlich ein bisschen Kartenleserei. Betrachten Sie die aktuell starke Volatilität als Geburtswehen eines neuen Systems, das sich settlet? Oder gehen Sie davon aus, dass es weiter nach oben geht und vielleicht sogar irgendwann abstürzt... und sich dann eventuell auf einem Wert festhält? #00:12:21-6#

Nigischer: Da kann ich keine unbeeinflusste Aussage treffen, da ich da zu stark drinhänge. Ich teile die Vision: Zielkurs 100.000. #00:12:33-9#

I: Dann hätte ich noch zwei weitere Fragen zur Akzeptanz. Damit Bitcoin relevant für Käufer ist, muss auf der Verkäuferseite auch diese Zahlungsmöglichkeit angeboten werden, genauso wie Käufer Bitcoin besitzen und als Zahlungsmittel nutzen möchten, damit der Verkäufer die Relevanz anerkennt. Das könnte man fast als einen Teufelskreis sehen. Wie schätzen Sie den Anstieg der Akzeptanz ein? #00:13:05-3#

Nigischer: Als Zahlungsmittel glaube ich, dass diese spezifische Blockchain-Variante Bitcoin in der Breite sich nicht durchsetzen wird. Eher für Use-Cases wie Wertspeicherung oder als Trading-Objekt, aber nicht für das tägliche bezahlen. Da haben wir... da haben wir einfach sehr, sehr gute Alternativen zur Verfügung, die gar nicht so sehr aus dem Bereich der Kryptowährungen kommen, wo jetzt aktuell... da sehe ich schon eine Entwicklung wo man sagt: „Wir verbinden die Entwicklung von Fiat-Geld mit den Möglichkeiten, die man bei Kryptowährungen sieht und wahrnimmt und schafft dort sehr sichere und kundenfreundliche Zahlungslösungen, die sich gut integrieren lassen in das, was die Leute heute schon gewohnt sind und die die Infrastruktur, die wir heute schon am Point of Sale nutzen. #00:14:07-1#

I: Haben Sie da ein Beispiel? #00:14:07-1#

Nigischer: Das Thema schnelle Mikrotransaktionen ist meiner Meinung nach gerade auf EU-Ebene umgesetzt worden, als technische Implementierung. Für sehr schnelle SEPA-Payments ist meiner Meinung nach auch etwas in der Mache. Also wo Überweisungen nicht Tage brauchen, sondern in Minuten durchgeführt werden. #00:14:34-9#

I: Meine weitere Frage dreht sich auch um die Massentauglichkeit von Bitcoin. Es gibt Public- und Private-Keys. Der Nutzer müsste sich dabei wenigstens etwas mit der Technik auseinandersetzen, wie er seine Bitcoins sichert. Da stellt sich mir die Frage: „Als wie massentauglich sehen sie Bitcoin unter diesem Aspekt an?" #00:14:57-1#

Nigischer: Ich glaube, dass das gar nicht die Frage ist, die man auf Bitcoin reduzieren sollte, sondern, dass IT-Security als wesentlicher Bestandteil um sicherzustellen, dass man sich in diesem Raum sicher bewegt etwas ist, dass wir in der Zukunft genauso brauchen wie Lesen und Schreiben. In der Ausbildung oder in der Schule müsste dieses Thema stattfinden, weil wir sonst als Gesellschaft ausgeliefert sind. #00:15:29-4#

I: Wobei das Thema IT in der Schule auch heute noch, behaupte ich einmal, sehr stiefmütterlich behandelt wird. #00:15:36-6#

Nigischer: Ja, das ist dramatisch. Das ist einfach total verantwortungslos. #00:15:41-2#

I: Würden Sie daher sagen, dass Bitcoin, oder Technologien mit kryptographischen Sicherheitsmechanismen nicht massentauglich werden? #00:15:51-8#

Nigischer: Also es wird gewinnen... wo fängt Massentauglichkeit an? Im Moment, vor allem durch die Kursgewinne, ist das Interesse einer zunehmend breiten Öffentlichkeit schon groß, aber die technischen Grundlagen... das ist ein langwieriger Prozess. Da müssen wir als Gesellschaft an sich und auch als Staat... da muss etwas passieren. Da muss mehr passieren. #00:16:24-1#

I: Mir ist noch eine Frage im Laufe des Interviews gekommen. Wie betrachten Sie die aktuellen politischen Auseinandersetzungen bei Bitcoin? In dem Fall bin auch nur über verschiedene Medien, wie beispielsweise Foren informiert, aber ich würde gerne Ihre Meinung hören. Bei Bitcoin Cash wurde dem

Entwicklerteam vorgeworfen, dass das eher eine Maßnahme war, Geld durch die Hardfork zu generieren. Oft wurde es als Angriff auf Bitcoin beschrieben. Ähnliches kann dem Bitcoin Ökosystem schaden. Wie schätzen Sie das ein? #00:17:00-8#

Nigischer: Ja, das Risiko besteht. Also wenn der Eindruck in der Bevölkerung entsteht, dass da Schindluder getrieben wird und dass das von wenigen wissenden und mächtigen ausgenutzt wird, dann kann das einen erheblichen Schaden für die langfristige Entwicklung nach sich ziehen. #00:17:18-3#

I: Alles klar, dann würde ich zu meiner letzten Frage kommen und zwar, als wie reguliert Sie Bitcoin aktuell einstufen und ob die deutsche Regierung sich diesem Thema bald auf gesetzlicher Ebene annimmt? Ich würde einmal behaupten, dass die deutsche Gesetzgebung oft in technischen Themen hinterherhängt. Glauben Sie, dass spezifische Maßnahmen noch kommen, die Bitcoin und andere Kryptowährungen betreffen? #00:17:39-1#

Nigischer: Ich könnte mir vorstellen, dass konkret zum Thema ICO, die Warnung dazu ist ja schon draußen, dass man da noch etwas nachlegt, wobei auch zusätzliche regulatorische Maßnahmen notwendig sind zu der konsequenten Anwendung des Rahmens, der heute schon besteht. Für Bitcoin an sich hoffe ich... ich glaube eher, dass es die Anwendung in der Praxis ist, wie mache ich richtig eine Steuererklärung usw. Ich glaube, dass der aktuelle Rahmen da ausreicht um damit zurecht zu kommen. Schädlich wäre eine zu frühe, oder eine übermäßige Regulierung, weil sie ja innovationshinderlich sein kann und weil der aktuelle Rechtsrahmen eine gute Basis bietet. #00:18:38-1#

I: Vielen Dank. Das waren alle meine Fragen. Ich bedanke mich. #00:19:47-6#

Anhang 4: Experteninterview Daniel Heller

Name	Daniel Heller
Aktuelle Institution	Peterson Insitute for International Economics (PIIE)
Funktionsbezeichnung/Titel	K.A.
Kontaktdaten	dheller@piie.com
Datum des Interviews	06.12.2017
Freigabe	nicht erforderlich

I: Ich möchte Sie anfangs einmal bitten sich vorzustellen, sowie die Berührungspunkte mit dem Thema, damit ich Sie in der Bachelorarbeit gut einordnen und als Experte vorstellen kann. #00:00:13-1#

Heller: Ich habe ein Doktorat in Volkswirtschaftslehre, dann ging ich zur Schweizer Nationalbank. Dort war ich zuerst in der Forschungsabteilung, habe dann die Abteilung „Payment System Policies“ aufgebaut. Da kam ich auch in Kontakt mit Systemrisiken, Großbetragsrisiken, aber auch Retail-Payments. Damals war gerade E-Money... die erste Welle von E-Money war populär in den 90er Jahren. Nachher habe ich mich etwas wegbewegt von diesem Thema hin zur Finanzstabilität... Risiken zwischen Banken und ging dann 2009... wurde ich dann Generalsekretär des *Commity on Payments and Settlement System*. Dort haben wir uns auch mit Innovationen im Zahlungsverkehr beschäftigt. Dann ging ich zum Internationalen Währungsfond [lacht]. Dort habe ich drei bis vier Jahre keinen Kontakt mehr zu Zahlungssystemen gehabt. Jetzt bin ich beim *Petersen Institute for International Economics*. Das ist ein Think-Tank und dort befasse ich mich jetzt mit digitalen Währungen, nicht zuletzt wegen Bitcoin. Das mache ich jetzt seit knapp einem Jahr. Quasi back to the roots. Damit habe ich vor 20 Jahren angefangen. Ursprünglich dachte ich Bitcoin is never going to work und dann verschwand das Thema nie. Da habe ich beschlossen, es genauer zu betrachten. #00:02:22-2#

I: Alles klar. Vielen Dank für die Vorstellung. Die nächste Frage ist eine einfache Frage und dient der Ableitung auf die nächsten Fragen. Bitte beschreiben Sie die zentralen Eigenschaften von Bitcoin und dessen Blockchain. #00:02:39-1#

Heller: Das ist relativ simpel. Es ist ein dezentrales, verteiltes System, welches Zahlungen Peer-to-Peer ermöglicht und ist die erste Anwendung dieser Art von Zahlungen. #00:02:56-8#

I: Vielen Dank. Dann möchte ich zur zweiten Frage kommen. Als was sehen Sie Bitcoin definitorisch? #00:03:08-5#

Heller: Es ist an sich ein Tauschmittel und geeignet als Zahlungsmittel. Als Recheneinheit sind sie eher ungeeignet, da es keine Zentralbank gibt, die den Wert konstant hält. Die Fluktuation ist viel zu hoch, um als Recheneinheit geeignet zu sein. Wertspeicherung... der Wert hängt eigentlich von der Funktion als Tauschmittel ab. Der nachhaltige Wert... da kommt es darauf an, wie populär es als Zahlungsmittel ist, und ob es zur Wertspeicherung dient. Von daher, Tausch-und Zahlungsmittel ist erfüllt, Recheneinheit ist nicht erfüllt und Wertspeicher ist unklar. Ist es eine Währung? Ich würde sagen nein. Die Kriterien sind nicht erfüllt. #00:04:53-7#

I: Sehen Sie es dann als Asset an? #00:04:5-7#

Heller: Ja, auf jeden Fall. Zum Thema Wertspeicherung... der Wert muss ja von irgendwoher kommen. Der Wert kann nicht... der einzige Weg, dass Bitcoin einen Wert hat, ist als Tauschmittel. Man muss etwas damit machen können, oder Pfad an sich kann keinen ökonomischen Wert haben. #00:05:26-5#

I: Der Wert wird ja durch den Markt bestimmt. Das wäre auch Frage fünf, da Bitcoin nicht von einer zentralen Entität geregelt wird, sondern sondern einzig durch den Markt selbst beeinflusst wird. #00:05:37-7#

Heller: Also es ist an sich eine... es ist auch so konzipiert, dass es ein Medium of Exchange darstellt. Es wurde einfach nur in ein Spekulationsobjekt mutiert. Aber an sich ist es ein Tauschmittel. Es ist also auch kein reines Asset. Man kann schon Vertrauen in das System haben, da die Geldmenge von einem Protokoll und nicht von einer Zentralbank gesteuert ist. Das ist eine gute Lösung. Aber es hat einfach den Nebeneffekt, dass man Schwankungen im Preis hat. Die Schwankungen gleichen der eines Assets und diese muss höher sein, als die einer Sovereign Currency. Die Nutzer müssen sich darüber im Klaren sein und bereit sein, das hinzunehmen. #00:07:12-3#

I: Das würde auch an die nächste Frage anschließen. Sehen Sie Bitcoin als wirtschaftlich an? Die Volatilität geht immer weiter nach oben. Ein Produkt könnte heute 100€ Wert sein, halte ich die Bitcoin aber, so könnte sich dies auf 150€ in absehbarer Zeit ausdehnen. Ist es daher wirtschaftlich, Bitcoin zu nutzen? #00:07:42-9#

Heller: Alle Studien zeigen, dass niemand Bitcoin verkauft, auch da wo man es brauchen könnte, wird es nicht eingesetzt. Was man sehen muss... ich meine, konventionelle Zahlungsmittel sind unglaublich schnell geworden. In der Schweiz können Retail-Payments in zwei Sekunden abgewickelt werden. Bitcoin dauert weitaus länger. Die Mining-Kosten sind natürlich auch verdammt hoch. Die Frage, die sich stellt lautet dabei, ob Bitcoin überhaupt Konkurrenz zu herkömmlichen Zahlungsmethoden darstellen kann? Die Fortschritte dort sind natürlich auch sehr groß. #00:09:47-7#

I: Ok, das würde auch gleich auf Frage sieben abzielen. Bitcoin muss ja, um Relevanz zu entwickeln, von beiden Seiten gefordert werden. Im Hinblick auf die Weiterentwicklung der traditionellen Zahlungsmittel, stellt Bitcoin da eine Alternative dar? #00:10:01-4#

Heller: Ich habe es einmal probiert, aber es ist nicht so ganz einfach bei Microsoft mit Bitcoin zahlen zu können. Wie Sie richtig sagen, es sind *Two-sided-markets.* Es ist nicht ganz einfach in den Markt reinzukommen. Ich glaube da geschieht relativ wenig im Moment, auch wenn große Firmen das anbieten. Ich würde einmal sagen die Wachstumsraten im Kreditkartenbereich sind immer noch weit größer. #00:11:43-4#

I: Ok, dann hätte ich eine weitere Frage zur Nutzung. Als wie massentauglich sehen Sie Bitcoin an? Der Nutzer benötigt ja ein wenigstens geringes technisches Verständnis über die Nutzung von Private- und Public-Keys. Wie schätzen Sie das ein? #00:12:02-9#

Heller: Wir sind natürlich noch immer im „early stage“ dieser Blockchain-Anwendungen und die werden sicher noch weitaus bedienfreundlicher in der kommenden Zeit. In fünf Jahren wird das sehr einfach sein. Die andere Frage ist wirklich, ob Bitcoin massentauglich sein kann. Da stellt sich die Frage des Kapazitätslimits des ursprünglichen Konzeptes. Wenn es mehr Verbreitung gibt, dann muss das Off-Chain passieren. Ich glaube nicht, dass das On-Chain möglich ist. Die Massentauglichkeit von Bitcoin ist On-Chain nicht gegeben. #00:13:08-3#

I: Es wird ja auch am Lightning-Network und anderen Lösungen gearbeitet, sowie weiteren Lösungen. #00:13:10-9#

Heller: Genau, man müsste da, aber das ist nicht die ursprüngliche Idee... Lightning ist powerful, aber es ist nicht Bitcoin, sondern ein zentrales System. #00:13:33-9#

I: Ok, dann wäre meine nächste Frage zur Nutzung, als wie sicher Sie die Nutzung über Wallets usw. sehen? #00:13:59-1#

Heller: Bitcoin ist sicher, aber die Schnittstellen, die Wallets, die Exchanges... die sind nicht so professionell aufgebaut wie herkömmliche Handelsplattformen. Die nehmen das einfach nicht ernst. Vielleicht wird eine Regulierung helfen. Das kostet aber auch viel Geld. Die Community hat da immer das Gefühl, alles ist viel günstiger. Wenn man sich die Downtimes anschaut, die Börsen sind oft sehr lange Offline. Das wäre natürlich für eine herkömmliche Handelsplattform nicht akzeptabel. Die haben Backups mit denen Sie innerhalb von fünf Sekunden auf ein komplettes Back-Up System wechseln können. Das ist eine ganz andere Liga. #00:15:35-2#

I: Genau die gleichen Erfahrungen habe ich auch gemacht. Die nächste Frage haben wir schon teilweise beantwortet, ich würde aber gerne noch einmal ins Detail gehen. Mir stellt sich die Frage, ob es auch abschreckend für Unternehmen ist, dass die Kunden nachvollziehen können, wie viel auf die Adresse eingegangen ist? Sehen Sie da Hemmschwellen für die Nutzung in Unternehmen? #00:15:54-1#

Heller: Die Anonymisierung ist ja relativ... man kann sich relativ gut schützen. Es ist eher ein Problem für beispielsweise Banken, die auf die Blockchain wechseln. Die haben eher diese Bedenken. Für Unternehmen oder Individuen sehe ich das nicht. #00:16:36-4#

I: Sehen Sie weitere Vor- und Nachteile bei der Nutzung von Bitcoin im Vergleich zu herkömmlichen Methoden? #00:17:14-9#

Heller: Zum einen ist Bitcoin bei den Kosten nicht konkurrenzfähig, beim Speed... da ist Bitcoin, vor allem im Retail-Bereich, gar keine Konkurrenz. Mit Lightning könnte dies anders werden. Der Punkt, wann sind Zahlungen nicht mehr umkehrbar, das dauert bei Bitcoin ungefähr eine Stunde, das ist auch zu lang. Wenn eine Bank 100 Millionen Euro überweist, dann will sie eine sofortige Bestätigung und nicht eine Stunde warten. Zusätzlich ist es probabilistisch. Bis man sicher eine Zahlung auf der Blockchain nachweisen kann, dauert es einfach zu lange. #00:18:16-5#

I: Meine nächste Frage dreht sich um die Stabilität. Wie schätzen Sie die Hard Forks ein, sowie die Auseinandersetzungen, die damit einhergehen? #00:18:25-#

Heller: Auf eine Art ist es ja nicht schlecht, wie Konsens in dem System gefunden wird. Aber jede Fork ist ein Eingeständnis, dass man einen Fehler in der Vergangenheit gemacht hat. Das System muss noch an den Punkt kommen, dass es das nicht mehr gibt, oder nur ganz selten. Ich habe allerdings eine Sympathie für die Art, wie es umgesetzt wird. #00:27:54-4#

I: Wie verhält sich Ihre Meinung in Bezug auf PoW. Die Energiekosten steigen immer weiter an und eine Zentralisierung ist in Sicht. #00:20-20-4#

Heller: Die Wahrscheinlichkeit einer 51% Attacke nimmt mit dem Steigen des Preises ab. Je nach Quelle sagt man, dass es vier große Pools gibt. Es gibt natürlich aber auch viele kleine Miner. Für mich ist die Energieverschwendung im Vordergrund. Ökonomen nennen das „Contestable Markets“. Die Marktzutrittsschranken sind relativ klein und es gibt „Economies of Scale“. Letztendlich wird der Wert gegen Null laufen. Es gibt mehr Miner, der Preis geht rauf, die machen vielleicht noch einen Gewinn, aber langfristig ist das nicht profitabel. Und es ist eine Verschwendung. #00:21:35-5#

I: Ethereum experimentiert ja gerade mit PoS. Das wäre ja eine andere Lösung. #00:21:40-9#

Heller: Genau, da werden wir sehen wie das funktioniert. Wenn schon, dann ist PoS sicher besser. #00:21:57-3#

I: Dann würde ich auch gleich zur nächsten Frage übergehen. Die IMF ist ja für die Wertstabilität von Währungen zuständig. Ich würde behaupten, dass im Krypto-Markt jetzt schon Manipulation stattfindet. Haben Sie da Bedenken, falls Bitcoin noch größer werden sollte? #00:22:27-5#

Heller: Ich glaube, auch wenn der Preis sehr hoch wird, wird Bitcoin nie eine große Rolle spielen. Und auf Währungen kann man sowieso nicht über mehr Bitcoin losgehen. Die interessante Frage ist die nach dem Systemrisiko. Was passiert bei dem Crash des Systems Bitcoin? Hat das Auswirkungen auf das Finanzrisiko? Ich glaube solange die Banken keine Bitcoin halten, solange der derivative Handel relativ gering ist, gibt es kein Systemrisiko. Heute könnte der Preis auf null sinken und es würde nichts geschehen. Weniger als 5% der Bitcoinhalter halten 95% der Bitcoins. Der marktökonomische Effekt ist klein. Wenn Banken in Bitcoin investieren, wenn es Auswirkungen auf die Bilanz hat, dann sehe ich Systemrisiken. #00:24:30-6#

I: Sehen Sie in Bitcoin eine Alternative zu Wertspeicherung wie über Gold? #00:24:37-6#

Heller: Würde ich nicht empfehlen [lacht]. Es gibt ja viele Leute, die sagen, sie wollen das als Diversifikation. Aber das funktioniert auch nicht immer. In den USA haben viele Leute in den Real-Estate investiert ,und die haben sie dann auch verloren. Einfach weil man diversifiziert, heißt das nicht, dass es auch einen Sinn ergibt. #00:25:24-8#

I: Ok, dann wären wir auch schon bei der letzten Frage. Wie reguliert sehen Sie Bitcoin an? #00:25:44-9#

Heller: Ich würde sagen: „Der Staat muss für Steuerzwecke einen Weg finden, dass diese Guthaben besteuert werden. Das ist ja jetzt nicht so schlecht über die Exchanges und Wallet-Provider geregelt. Die sollten ja wissen, wer diese Bitcoins hält. Auch die internationalen Regeln sind klar. Es ist einfach die Implementierung, die noch nicht erfolgt ist. In den USA wissen die, wer ich bin, Coinbase weiß, wer ich bin. Die können das an sich auch dem Finanzamt weitergeben. Mehr braucht es eigentlich nicht. Bei Banken muss man sich überlegen, ob es für diese verboten wird Bitcoins zu halten, oder ob es ein sehr hohes Risikogewicht bekommt. Wie gesagt, für Bitcoin müssen die AML, die Anti-Money-Laundering Provisions, die müssen durchgesetzt werden und die Exchanges müssen sich damit arrangieren. Das werden sie nicht gerne tun, da es etwas kostet, aber das wird kommen. Da bin ich sicher. #00:27:51-1#

I: Vielen Dank. Das waren alle Fragen. #00:27:58-5#

Anhang 5: Experteninterview Florian Fiedler

Name	Florian Fiedler
Aktuelle Institution	Blockbay
Funktionsbezeichnung/Titel	Geschäftsführer
Kontaktdaten	Stadthausbrücke 1-3
	20355 Hamburg
	florian.fiedler@blockbay.de
Datum des Interviews	28.11.2017
Freigabe	nicht erforderlich

I: Um Sie in meiner Bachelorarbeit besser einordnen zu können, möchte ich Sie am Anfang bitten, sich ganz kurz einmal vorzustellen, wie schon im Leitfragebogen angedeutet, Ihre derzeitige Tätigkeit und was so die Berührungspunkte mit dem Thema sind. #00:00:13-1#

Fiedler: Gerne, ich fange einmal chronologisch an. Ich komme aus der klassischen Management- und Strategieberatung. Dort habe ich über viele Jahre auf Vorstandsebene Projekte für Banken im In- und Ausland durchgeführt bzw. geleitet. Mit dabeiwaren auch die Gründung einer Bank, der Verkauf einer Bank und Merger zwischen Banken. Von dort aus bin ich in die Konzernstrategie von IBM in Deutschland, Österreich und der Schweiz gewechselt. Dort haben wir u.a. die Geschäftsstrategie entwickelt und ein neues Vertriebskonzept erstellt. Von dort aus bin ich zur HSH-Nordbank gewechselt, in den Strategiebereich. Fokus waren strategische Restrukturierungsprojekte, mit denen wir im Ergebnis den Verwaltungsaufwand der Bank um 50% reduzieren konnten, aber auch die Neuausrichtung des Firmenkundengeschäfts. Dann war ich bei der HSH als „Head of Digital Business“ analog zur Funktion eines Chief Digital Officer tätig, und habe die Digitalisierungsthemen der Bank verantwortet und vorangetrieben. Zu Beginn kam dabei die Frage vom Vorstand: „Was ist eigentlich Bitcoin?“ So haben wir in der Thematik relativ schnell festgestellt, es ist eigentlich nicht Bitcoin, sondern die Blockchain, die für Banken besonders relevant ist. Wir haben uns der Thematik sehr stark angenommen und auch ein Projekt zur Implementierung der Blockchain in der Bank... gestartet und umgesetzt. In dem Zuge haben wir durch die Berührungspunkte mit der Blockchain sehr schnell festgestellt, was da für große Potenziale dahinterstehen. Dann habe ich in diesem Jahr zusammen mit Partnern ein eigenes

Unternehmen gegründet, um diese Potenziale als Start-Up noch besser ausnutzen zu können. Die Umsetzung von innovativen Geschäftsideen ist als Startup noch wesentlich einfacher, schneller und flexibler möglich als in einer etablierten Bank. #00:02:25-3#

I: Was genau macht Ihr Unternehmen? Ich habe auf der Webseite einmal geschaut, aber mir war dabei nicht so ganz klar, was Ihr Bereich ist. #00:02:30-5#

Fiedler: Dann haben wir das Ziel erreicht, denn genau das wollen wir noch nicht verraten. Wir sind noch in der Vorbereitungsphase. Nächstes Jahr wird das Produkt live gehen. Bis dahin wollen wir aber keine Wettbewerber aufschrecken. Wir denken wir haben da eine First-Mover-Advantage mit dem, was wir hier machen. Insofern wird das Geschäftsmodell auf der Website absichtlich noch nicht weiter konkretisiert. Es wird eine Plattform für Trader von Kryptowährungen, Bitcoin ist eine davon, aber da gibt es noch eine Menge andere. Ich verrate nicht viel aber wir werden den Händlern das Leben deutlich einfacher machen... ihre Aktivitäten können diese dann deutlich effizienter durchführen, wenn sie uns nutzen. Wir versuchen dabei den traditionellen Reifegrad der Finanzmärkte auf die Kryptowelt zu übertragen. Da gibt es noch eine Vielzahl ungenutzter Potenziale. #00:03:51-4#

I: Ok, vielen Dank. Dann würde ich sagen wir gehen auf die erste thematische Frage ein, damit wir die weiteren Antworten davon ableiten können. Ich möchte Sie einmal kurz bitten die zentralen Eigenschaften der Blockchain aufzuzählen. #00:04:03-5#

Fiedler: Ja, ich habe mir dazu ein paar Notizen gemacht. Das ist natürlich sehr einfach. Die zentrale Eigenschaft ist, dass es nicht zentral ist. Also *Dezentral* ist eine Eigenschaft. Man kommt ohne Intermediäre aus, ohne Banken, oder auch in anderen Industrien kann ein etwaiger Intermediär komplett ersetzt werden durch die Nutzung einer Blockchain. Sicher, non-reversibel, nicht unter sinnvollem Aufwand manipulierbar oder korrumpierbar. Auch, aufgrund der Dezentralität... es wird nichts zentral gesteuert durch eine Regierung oder eine andere zentrale Partei, sondern es ist eben komplett dezentral. #00:04:53-4#

I: Perfekt, danke. Dann würde ich auch gerne auf die Nutzung eingehen. Für wie sicher halten Sie die Nutzung von Bitcoin, abgesehen von der Blockchain, die ja seit sieben Jahren nicht gehackt wurde, über ihre Schnisttellen, wie die Wallets. Vor allem bei den Software-Wallets. Bei Ethereum gab es ja letztens, wie Sie...

ach ja Sie hatten mir ja das Du angeboten, wie du vielleicht mitbekommen hast, einen Bug, bei dem 150 Millionen eingefroren wurden. Für wie sicher hältst du die Nutzung von Bitcoin daher? #00:05:18-8#

Fiedler: Ähnlich. Vielleicht ist es ein bisschen sicherer als neuere Währungen, bei denen die Technologie noch nicht ganz so ausgereift ist. Aber da muss man glaube ich ganz klar differenzieren. Ich halte die Blockchain-Technologie an sich für extrem sicher. Wie vorhin schon gesagt kann man ja auch aus einem Hash, der als nicht umwandelbar gilt, das Passwort generieren. Kann man theoretisch schon, allerdings nicht mit Vernünftigem Aufwand. Das wird für Hacker immer irrational bleiben das zu versuchen. Die kann man nicht unter vertretbarem Aufwand hacken, die Technologie, aber in der Anwendung, genau wie du sagst, gibt es aus meiner Sicht zwei wichtige Punkte. Und zwar, zum Einen in der individuellen Nutzung kann der Nutzer... wenn er ein Paper-Wallet hat kann er dies verlieren, oder wenn er alles auf einem USB-Stick gespeichert hat oder in einer Software kann er das verlieren. Das Passwort kann man auch verlieren. Da ist man natürlich eine Gefahr bei der Nutzung, anders als wenn man dies auf einem Bankkonto hat, dass man auf einmal nicht mehr auf das Geld zugreifen kann. Das Gleiche ist, dass eben solche Wallets oder auch Börsen auch gehackt werden können. Das liegt dann wieder nicht an der Blockchain-Technologie, sondern da haben die Börsen ihre Hausaufgaben nicht gemacht. MT. Gox wurde gehackt, Bitfinex wurde sogar zweimal glaube ich gehackt. Das liegt dann aber nicht an der Technologie, sondern eben an den Börsen. Vielleicht noch eine Anmerkung, wenn man im großen Stil an Börsen hackt, kann man mit dem erbeuteten Krypto-Geld anschließend nichts anfangen. Sie können es klauen, es wird aber jeder sofort merken, wie bei Gelscheinen die markiert sind, diese Bitcoin oder diese Ether sollte ich nicht annehmen, weil sie aus einem Hack stammen. Warum wird es trotzdem gemacht? Sie erinnern sich an den Anschlag auf die Mannschaft von Borussia Dortmund, der Attentäter hat vorher den Kurs der Dortmund-Aktie geshortet. Sprich, wenn wir heute Abend jetzt irgendeine große Krypto-Börse hacken, dann können wir mit dem was wir verdienen, also was wir erbeuten nichts anfangen, aber mit der Wette auf den Kurs... dann haben wir darüber etwas verdient. #00:08:07-3#

I: Vielen Dank. Der nächste Punkt wäre, dass Zahlungen nicht rückgängig gemacht werden können. Sehen Sie dabei Vor- und Nachteile für Unternehmen oder auch Endkunden? #00:08:15-3#

Fiedler: Vor- und Nachteile, beides. Ein Vorteil ist eben, dass alles, das in der Blockchain eingetragen ist, nicht mehr reversibel ist. Blockchain hat ja auch, oder

Bitcoin hat ja auch häufig ein schlechtes Image, dass kriminelle damit Zahlungen tätigen. Das würde ich als Krimineller niemals tun, denn es steht irreversibel und auf alle Ewigkeit in der Blockchain drin, wann, wo, wie, welche Transaktion in der Blockchain stattgefunden hat. Das kann man im Rahmen der Strafverfolgung durchaus, wenn man die Daten hat, mit einem gewissen Aufwand wer das denn war. Das wurde ja auch schon einmal gemacht. Das heißt, das ist, denke ich, ein großer Vorteil. Auch in anderen Anwendungsfällen kann man die Originalität von Dingen nachweisen. Das macht das Ganze fälschungssicher. Das hat aber natürlich den Nachteil, wenn ich jetzt an ein anderes Wallet, also ich schulde dir ein Bitcoin und möchte ihn überweisen, aber ich vertippe mich und mache aus einem X aus Versehen ein Y, dann kommt der Bitcoin woanders an und ich kann ihn mir nicht zurückholen. Ich kann den anderen anschreiben, wenn ich es überhaupt hinbekomme ihn zu kontaktieren, und ihn bitten mir meinen Bitcoin zurückzugeben. Aber dieser muss das nicht tun. Das ist natürlich ein gewisser Nachteil. Da sollte man überlegen mit einem Vier-Augen-Prinzip zu arbeiten, vor allem bei einer größeren Überweisung. Börsen haben da Copy-Paste Funktionen oder Adressbuchfunktionen, die machen das leichter, aber das Risiko ist auch da immer noch vorhanden. #00:10:03-3#

I: Dann würde ich gleich bei den Transaktionen bleiben, die ja schon fast den Kerngedanken der geringen Gebühren und der Dezentralität kaputt machen. Wie ordnen Sie diese für Bitcoin als Handelswährung ein? Das Lightning-Network soll eingeführt werden, aber auch schon länger. Sehen Sie da Probleme? #00:10:24-4#

Fiedler: Es kommt ein bisschen darauf an, wofür man Bitcoin nutzen will. Ich denke, man kann etwas tun, man kann etwas verbessern. Dafür muss man später aber auch einen Konsens haben, zwischen den wichtigen Parteien, die sich entscheiden das einzuführen. Es wird, glaube ich, bei Bitcoin niemals so weit verbessert werden, dass Transaktionen im Massenvolumen, vergleichbar zum Beispiel mit VISA... mit Kreditkartenzahlungen ermöglicht werden. VISA hat vor längerer Zeit die Blockchain schon einmal getestet. Ja, man kann damit alles wunderbar abwickeln, aber die Anzahl an Transaktionen, die werden Sie, zumindest in der Bitcoin-Blockchain, das ist so meine Prognose, niemals abwickeln können. Dafür gibt es andere virtuelle Währungen, die entweder auf der Blockchain, manchmal aber auch auf weiter entwickelten Versionen dieser, wie dem *Tangle*, basieren. Da gibt es Technologien, die komplett ohne Transaktionskosten auskommen, wo so etwas tendenziell auch sehr schnell möglich ist und auch *Micropayments* ermöglicht werden. Deshalb, mit diesen langen Transaktionszeiten und auch mit diesen hohen Transaktionskosten, die Du

angesprochen hast, mit ungefähr fünf Dollar pro Transaktion, wird es niemals Sinn ergeben, ein wichtiger Irrglaube, den man glaube ich einmal ausräumen muss, einen Kaffee bei Starbucks mit Bitcoin zu bezahlen. Das macht man vielleicht einmal aus Spaß, aber dann zahlt man für seinen Kaffee, der fünf Dollar an Starbucks plus fünf Dollar an Transaktionskosten. Die Durchführung einer solchen Transaktion ist demnach oftmals unwirtschaftlich. #00:12:12-2#

I: Ungefähr 10 Minuten. #00:12:13-4#

Fiedler: Danke, 10 Minuten oder länger darauf. So lange möchte ich nicht vor der Kasse warten, bis die sagen: „Ja, danke. Ist angekommen." Dafür ist es nicht sinnvoll, aber für andere Use-Cases. #00:12:25-9#

I: Dann würde ich schon einmal eine Frage vorgreifen und zwar, ob Sie ein Problem mit dem, immer zentralisierteren Proof-of-Work sehen. Proof-of-Stake wird ja aktuell bei Ethereum getestet. #00:12:38-9#

Fiedler: Ich bin kein Techniker, gehe aber mit meinem rudimentären Verständnis davon aus, dass Proof-of-Stake Abhilfe schafft und auch, dass es das bessere und fairere Verfahren ist. Aber wie gesagt, das ist mein Laienverständnis. Ich bin da jetzt nicht absolut in der Tiefe drin und habe mir die Algorithmen angeschaut. Da gibt es Experten, die diese Frage fundierter beantworten können. #00:13:13-0#

I: Zu der Zentralisierung. Es gibt ja immer weniger Mining-Pools, die da quasi die Oberhand haben. Haben Sie da Angst vor Absprachen? #00:13:21-1#

Fiedler: Ja, das ist natürlich schon ein Thema. Die Miner bekommen immer mehr Macht. Es gibt andere Kryptowährungen, da kann man, sag ich mal, mit einer Grafikkarte minen. Da gibt es Leute, die haben auf der Welt 10 Rechner stehen und minen damit. Wenn sie aber immer zentralisierter werden und Mining-Parks oder Rechenzentren haben, in denen nichts anderes als Mining betrieben wird und in allen anderen Ländern sich das nicht lohnt... vor allem für Kleinanbieter, weil der Strompreis zu hoch ist und das Ganze in kleinem Umfang einfach nicht wirtschaftlich ist, dann finde ich, das ist im Stück weit gegen den Dezentralen Gedanken. Ich empfinde das nicht, jedenfalls nicht im Moment, als großes Problem, aber es ist tendenziell keine gute Entwicklung. #00:14:10-5#

I: Danke, dann würde ich noch einmal darauf eingehen, als wie fragil Sie das System einschätzen. Es gibt ja Miner, Nodes und Entwicklerteams, die ja schon einen kleinen und elitären Kreis bilden, der über die Zukunft von Bitcoin bestimmt. Wie schätzen Sie das ein? #00:14:28-7#

Fiedler: Also, meiner Wahrnehmung nach ist es so, dass es vielleicht sogar stabiler ist, als es sein sollte. Teilweise hemmt diese Situation vielleicht sogar den Fortschritt, weil sich diese Parteien häufig nicht ganz einigen können. Soll eine größere Blocksize eingeführt werden oder nicht? Manche sind dafür, andere dagegen. Dann gibt es diese Hard-Forks und die bringen wiederum eine große Unsicherheit mit sich. In der Vergangenheit war es häufig so, dass dann beide Währungen koexistierten und der Wert der neuen Währung dann auf die Marktkapitalisierung, also auf den Wert der alten Währung, obendrauf kam. Auf einmal war dann Bitcoin das 1,2-fache Wert. Rein wirtschaftlich finde ich das sehr schwer nachvollziehbar. Ich finde das, was man neu bekommt, sollte man vom Alten abziehen. Die aktuelle Marktreaktion auf derartige Forks halte ich im Moment für eine etwas irrationale Reaktion, also sehr spekulativ getrieben. Und auch sehr verwirrend für Endnutzer. Dann gibt es Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond. Wenn jetzt der, ich sage einmal gemeine Endnutzer darauf kommt und sich noch nicht so damit auseinandergesetzt hat, dann kauft er vielleicht einfach ein paar Bitcin Cash, anstatt Bitcoin. #00:16:08-2#

I: Das wäre auch meine nächste Frage gewesen. Dann springe ich zur nächsten Frage. Ich weiß nicht, wie sehr sie das mitbekommen haben, aber es gab ja ein paar politische Auseinandersetzungen zwischen dem Core Team und dem Cash Team. Viele sagen dem Cash Team dabei nach, die Hardfork nur als Gelddruck gestartet zu haben. Es gab auch keine Replay-Protection im Code, also dass beim Senden von Bitcoins aus dem Wallet aus Versehen ungewollt auch Bitcoin Cash mitgesendet werden kann. Wie sehen Sie das, das alles von so einem kleinen Kreis abhängt? #00:16:26-7#

Fiedler: Ich kann keine fundierte Antwort darauf geben. Ich muss für mich persönlich gestehen, dass ich bei diesen Fork-Diskussionen in der Regel ausgestiegen bin und nicht alles im Detail nachverfolgt habe. Für mich habe ich nur entschieden ob es sinnvoll ist oder nicht. In der Regel war ich kein großer Fan der Fork und habe beschlossen, auch in diese nicht zu investieren. Mir fehlt einfach die Zeit, den Diskussionen technisch zu folgen, um hier eine gute und fundierte Antwort zu geben. #00:17:17-7#

I: Ok, dann fahre ich mit der nächsten Frage fort. Durch die Transparenz des Netzwerks ist ja alles nachvollziehbar. Stellt das Vor- und Nachteile für Unternehmen dar? Schreckt das vielleicht sogar Unternehmen ab, wenn man weiß, was wieviel auf welche Adresse eingegangen ist? #00:17:34-8#

Fiedler: ...Ja, eine gute Frage. Das ist ein sehr guter Punkt. Also normalerweise sind das natürlich Vorteile. Man kann alles, wie vorhin gesagt, grundsätzlich nachvollziehen. Es geht ja auch nicht immer alles um Zahlungen. Blockchain ermöglicht ja den Wertetransfer und das kann auch eben sein, dass ich meinen Fahrzeugbrief jemand anderem, Zwecks Verkauf, gebe und dies über die Blockchain abwickle. Da ist es ein riesen Vorteil, dass hierbei eine Transparenz besteht. Wenn jemand behauptet, hier gab es nur zwei Vorbesitzer, dann kann ich das darüber prüfen und sagen: „Moment, hier in der Blockchain sind aber fünf eingetragen, das stimmt so nicht. Da entsteht natürlich ein riesen Vorteil. #00:18:24-4#

I: Übertragen auf Bitcoin könnten Nutzer so zum Beispiel nachweisen, dass sie Zahlungen getätigt haben? #00:18:31-2#

Fiedler: Richtig, das stimmt. Das ist auf jeden Fall ein Vorteil. Dem Finanzamt gegenüber, da existiert ja eine diffizile Steuerthematik hier in Deutschland, anders als in der Schweiz. Dort ist das einfacher. Da hilft das dann auch sehr, wenn man weiß, es ist irreversibel gespeichert. Selbst, wenn ich es mir gerade nicht in meiner Excel-Datei oder in meinem System gespeichert habe, kann ich es im Zweifel nachträglich rekonstruieren und dann noch einmal genau gucken wann ich was wann verkauft habe und welche etwaigen Gewinne und Verluste ich gemacht habe. Ein Nachteil, genau wie du sagst, kann bestehen, wenn ich eine Bitcoinadresse habe und ich lasse mir über zwei Jahre lang mein gesamtes Gehalt durchgehend, beispielsweise als Freelancer, schicken, dann kann jeder, der die Adresse hat, schauen, was die Menschen vor ihm gezahlt haben. Das ist aber nicht besonders schlau von dem Nutzer. Man kann jeweils immer eine neue Adresse generieren, was auch zu empfehlen ist, wenn man nicht alles offenlegen möchte, welche Transaktionen stattgefunden haben. Es ist zwar in der Blockchain gespeichert und man kann die Vorteile nutzen, man muss aber nichts von sich selber preisgeben. #00:19:58-2#

I: Einige Wallets machen dies ja sogar automatisch. #00:20:00-4#

Fiedler: Richtig. #00:20:03-1#

I: Ok, dann würde ich jetzt auf die nächste Leitfrage eingehen. Eine Währung muss ja drei Kriterien erfüllen: Tausch- und Zahlungsmittel, Recheneinheit und Wertspeicher. Würden Sie Bitcoin als Währung einstufen? #00:20:17-2#

Fiedler: Fangen wir beim ersten an. Tausch-und Zahlungsmittel...eingeschränkt. Teilweise kann es durchaus sinnvoll sein, beispielsweise als Gastarbeiter zurück in die Heimat zur Familie statt via herkömmlicher Anbieter mit sehr hohen Transaktionsgebühren und Wartezeiten, den erarbeiteten Wert über Bitcoin zu verschicken. Da sind diese fünf Dollar Gebühren immer noch viel geringer und Bitcoin in dem Fall ein super Zahlungsmittel. Es ist grundsätzlich ein super Tauschmittel, aber eben absolut nicht massenkompatibel. Es wird niemals, wenn wir jetzt einmal bei Bitcoin bleiben, eine der klassischen Währungen ablösen. Es wird keine Weltwährung, oder Weltersatzwährung werden oder den Dollar oder den Yen jemals im täglichen Leben ablösen können, weil einfach sehr hohe Transaktionsgebühren und -zeiten dazu kommen und es eben nicht so hoch skalierbar ist, wenn wir nur bei Bitcoin bleiben. Ich gehe dann noch einmal auf B und C ein (Anmerkung des Autors: Die weiteren beiden Kriterien). Recheneinheit... würde ich auch sagen eingeschränkt. Grundsätzlich ja, wenn Sie sich einmal anschauen, es existieren ca. 1350 virtuelle Währungen... nicht alle werden gegen US-Dollar getraded, aber alle wichtigen gegen Bitcoin. Insofern ist das eine super Recheneinheit, wie viel Bitcoin ist mein anderes Investment wert? Bitcoin ist dabei, innerhalb der 1300 die wahrscheinlich stabilste Währung, obwohl sie immer noch sehr volatil ist. Das heißt, ich kann ein Investment in *IOTA* (Anmerkung des Autors: eine Kryptowährung) machen und immer prüfen, wie viel habe ich denn jetzt in Bitcoin als Recheneinheit und habe ich in Bitcoin auch performt, oder nicht? Das ist so, wie als wenn sie eine Aktie kaufen und gucken, bin ich besser als der DAX oder nicht? Oder ich kaufe Aktien der Commerzbank und gucke, haben sie sich besser entwickelt als die der Deutschen Bank, das wäre ein passenderes Beispiel. Also Recheneinheit eingeschränkt, aus dem Grund, dass sie sehr volatil ist. Anders als bei dem Gold oder dem Dollar, bei denen die Schwankungen viel geringer ausfallen. Wenn der Preis an einem Tag um 20% schwankt, da stellt sich die Frage wie gut sich Bitcoin als Recheneinheit eignet. Zum Thema C, also Wertspeicherung, da würde ich sagen: „Das ist voll erfüllt." Wenn man sich jetzt einmal andere Länder anschaut und nicht die großen Industrienationen, sondern ein Land wie Venezuela oder andere Länder in Südamerika, dann wird dort häufig der Landeswährung nicht vertraut. Das ist auch ein Nachteil von den Zentralbanken, es bestehen ja nicht nur Vorteile, die können ja nach Belieben Geld nachdrucken. Dadurch entsteht dann oft eine riesen Inflation und wenn die Leute, im Gegenwert, ein Gehalt von 1000 Dollar bekommen, und im nächsten Monat ist das nur noch 800 wert, oder noch weniger. Und um sich davor zu schützen,

in diesen Ländern, ist dies ein wunderbares Wertspeicherungssystem. Da kann die Regierung einem keinen Strich durch die Rechnung machen. Ich bin noch nicht einmal abhängig vom Dollarkurs. Ja, ich habe die Volatilität des Bitcoins, aber im Vergleich zu dem Risiko, dass meine Regierung mit meinem Geld Schabernack treibt, nehmen viele die Volatilität in Kauf und sehen darin viele Vorteile. In Deutschland, Wertspeicherung ja, allerdings nur bei Technologieaffinen und Blockchain-Enthusiasten. In der breiten Masse noch eher schwierig. #00:24:37-9#

I: Also, würden Sie Bitcoin eher als Asset mit währungsähnlichen Eigenschaften einordnen? #00:24:53-4#

Fiedler: Anders als diese ganzen anderen 1300, die eher Start-Ups ähneln oder andere Funktionen erfüllen, würde ich schon sagen: „Bitcoin ist eine gewisse Währung." Es macht sicherlich auch Sinn, wenn man jetzt ein größeres Vermögen hat einen kleinen Teil dieses Vermögens in Bitcoin investiert zu haben. Einfach um zu diversifizieren. #00:25:39-3#

I: Ok, dann würde ich einmal weg von den Definitionen und hin zur Stabilität schwenken. Bitcoin besitzt ja keine zentrale Entität, wie die EZB beispielsweise, und ist quasi ein System, das auf dem Vertrauen der Nutzer in dieses basiert. Als wie stabil schätzen Sie das daher ein? #00:25:59-6#

Fiedler: Das System sehe ich grundsätzlich als sehr stabil an. Wir sind aber... das ist sehr wichtig... der Handel von Bitcoin ist lange nicht so ausgereift, wie der Handel von anderen Währungen, wie dem Dollar, dem Euro oder Rohstoffen usw. Aber weil der Handel noch so in den Kinderschuhen steckt, sind dort dementsprechend auch noch viele Risiken drin. Insbesondere diese Volatilität, die ja im aber im Vergleich zu den letzten Jahren schon stark abgenommen hat, aber dennoch ein vergleichsweise Vielfaches beträgt. #00:26:56-1#

I: Ok. Um noch einmal auf die Volatilität einzugehen. Ich kann ja als Nutzer sagen: „Oh, ich habe drei Bitcoin, die sind heute 600 Dollar wert, könnten aber morgen 700 wert sein. Kaufe ich mir etwas dafür oder warte ich lieber, wenn die Gefahr besteht, dass ich heute ein Produkt für 600 Dollar kaufe und meine Bitcoin zum Zeitpunkt des Eintreffens vielleicht aber schon 700 oder sogar 800 wert sein könnten?" Sehen Sie da eine Hemmschwelle für die Wirtschaftlichkeit Bitcoins? #00:27:15-6#

Fiedler: Ja, auf jeden Fall. Wie du gerade schon gesagt hast, es ist ja eben Spekulation. Man spekuliert auf einen steigenden Preis. Das kann man machen, würde ich aber trennen vom Praxiseinsatz. Wenn ich mir ein Produkt damit kaufen möchte, dann möchte ich ungefähr vorher wissen, was ich für dieses Produkt ausgebe. Und wenn ich immer vorher nachschauen muss und eventuell feststelle, dass mein Produkt in den letzten 10 Minuten 10 Euro teurer geworden ist, dann würde ich das im Endeffekt als Nutzer nicht positiv sehen. #00:27:54-1#

I: Alles klar. Dann möchte ich noch einmal auf die Massentauglichkeit eingehen. Wir haben ja in diesem Interview schon festgestellt, dass einige Eigenschaften einer Massentauglichkeit stark entgegenwirken. Die Nutzer müssen sich ja mit den technischen Eigenschaften auskennen und wissen, was Private- und Public Keys sind, um sich sicher im Ökosystem zu bewegen. Sehen Sie da eine große Hürde und eventuell einen Lernprozess, der noch vor den Menschen liegt? Ist dieser überhaupt notwendig? #00:28:16-6#

Fiedler: Ich würde hierbei zwischen privaten Endnutzern und Unternehmen differenzieren. Wenn Unternehmen große Handelswährungen verwenden, dann ist das glaube ich kein Thema. Das können die nach einer entsprechenden Mitarbeiter-Schulung wahrscheinlich schnell professionell einsetzen. Wenn Sie in einem Unternehmen den Mitarbeitern die Verwendung komplexer IT-Systeme wie z.B. *SAP* zutrauen, dann können diese Mitarbeiter nach einer Schulung und innerhalb klar vorgegebener Prozesse auch mit Bitcoin hantieren. Wenn wir jetzt bei den Endnutzern bleiben, dann ist das heute noch so, dass man eine gewisse technische Affinität mitbringen muss, was auch sehr viele noch von der Nutzung abhält. Ich kenne persönlich viele, auch aus dem Bankenumfeld, die zwar sagen, dass es für sie sehr sinnvoll sein könnte, aus Spekulationsgründen, ein paar Bitcoin zu kaufen, es aber niemals umgesetzt haben, weil sie gesagt haben: „Ich traue mir das nicht zu, oder ich habe nicht die Zeit mich in das Thema umfassend einzulesen, damit ich es so gut verstehe, dass ich es die Transaktion sicher abwickeln kann." Deshalb halte ich es für sehr wichtig und sinnvoll, dass diese Hürden gesenkt werden. Das können wunderbar Banken machen. Die Bank „Vontobel" hat beispielsweise ein Zertifikat ausgegeben, da kannst du als Bankkunde hingehen und sagen: „Ich habe ein paar tausend Euro übrig und mit denen möchte ich ein bisschen spekulieren. Ich würde gerne an der Bitcoinpreisentwicklung partizipieren, aber ich traue mich nicht ein eigenes Wallet zu kreieren usw." Das übernimmt dann die Bank und speichert auch die Bitcoins auf einem USB-Stick bei denen im Tresor. Solche Angebote sollten noch mehr kommen,

um die weniger technikaffinen Personen, die nicht die EarlyAdopters sind, auch mit ins Boot zu holen. Ich glaube, da ist noch ein großes Potenzial vorhanden. #00:30:40-9#

I: Also sehen Sie für Banken auch neue Geschäftsfelder aufkommen. Ein bisschen zurück zu dem ursprünglichen Gedanken von Banken als Wertspeicher, also diese für den Nutzer Bitcoin akquirieren und lagern? #00:31:01-5#

Fiedler: Ja, auf jeden Fall. Das ist ein Use-Case. Es gibt für Banken noch viele Use-Cases, insbesondere mit der Blockchaintechnologie, aber das ist auf jeden Fall einer davon. #00:31:11-9#

I: Dann hätte ich noch eine Frage zu Akzeptanz. Wenn mehr Händler Bitcoin als Zahlungsmittel anbieten, dann haben im Umkehrschluss ja im Idealfall auch mehr Nutzer Interesse. Wenn mehr Nutzer Interesse zeigen, dann sehen Unternehmen eine ansteigende Relevanz in Bitcoin als Zahlungsmittel und bieten dieses eventuell an. Das ist ja quasi ein Teufelskreis, bei welchem es auf einer oder auf beiden Seiten beginnen muss. 2017 war ein medial starkes Jahr für Bitcoin. Wie schätzen Sie dies ein? #00:31:33-7#

Fiedler: Akzeptanz... also bei Amazon und Microsoft wird ja diskutiert, ob sie Bitcoin annehmen. Rein ökonomisch betrachtet halte ich es für nicht opportun das zu tun. Ich halte es für einen Marketinggag, vor allem aufgrund der genannten Transaktionsgebühren und -zeiten. Es wird aber sicherlich irgendwann eine Kryptowährung geben, die diese Probleme besser im Griff hat, oder gar nicht mehr aufweist. Bei dieser kann es dann sehr viel Sinn ergeben, damit zu zahlen. Bei Bitcoin sehe ich das ehrlich gesagt nicht. #00:32:13-3#

I: Sehen Sie künftige Maßnahmen Staates Bitcoin, oder Krypto-Assets im Allgemeinen, stärker zu regulieren? Ich habe jetzt schon einige Interviews geführt und festgestellt, dass es schon einige bereits bestehende Regulierungen gibt, die auf dieses Thema bezogen werden oder bezogen werden können. Sehen Sie noch spezifische Ansätze kommen? #00:32:32-8#

Fiedler: Ich bin mir sicher, dass da noch einiges kommen wird. Gerade die Regulierung ist noch in den Kinderschuhen, aber ich denke, dass die Welt da aktuell ein Stück aufgewacht ist. Die SEC in den USA hat sich die ICOs genau angesehen und geprüft, ob es sich um Securities handelt. Wenn ja, dann sind bestimmte Regeln zu befolgen.

Die Schweiz hat dazu etwas veröffentlicht und die BaFin, die Aufsichtsbehörde in Deutschland für die Banken, hat vor drei Wochen ein Statement dazu abgegeben, dass tendenziell sagt, dass man aufpassen muss, ob man das darf oder nicht. Ich glaube, es werden noch eine Menge Regulierungen kommen und ich glaube, dass Regulierung etwas Gutes ist. Da muss man wieder auf den Kontext aufpassen. Insbesondere bei den ICOs sehe ich Regulierung als gut an und auch in Bezug auf andere Kryptowährungen, weil es Handlungssicherheit schafft. Wenn Du heute als Unternehmen einen Freelancer aus einem anderen Land einstellst und dieser die Internetseite programmiert und sagt: „Bezahl mich bitte in Bitcoin.“, dann erzähl das mal deinem Steuerberater. Das kriegt der nur unglaublich schwer in der Bilanz abgebildet. Genauso kannst du nicht Dienstleistungen anbieten und dich in Bitcoin bezahlen lassen, weil der Steuerberater ein riesen Problem damit hat. Es ist zwar in Deutschland geklärt, wie alles zu versteuern ist, aber das ist da nur Beispiel um einmal zu erklären, wichtig es ist, dass man klare Regeln und Rechtssicherheit hat. #00:34:37-6#

I: Alles klar. Das wären eigentlich alle meine Leitfragen. Eine ist mir noch während des Interviews gekommen. Hätten Sie noch Zeit? #00:34:46-1#

Fiedler: Ja, gerne. #00:34:46-2#

I: Sie kommen ja aus dem Bankenwesen und kennen dann sicher auch spekulative Attacken auf Währungen. Da ist mir die Frage gekommen... die IMF hat ja den Zweck, durch Währungen aus allen Staaten die da mitmachen, das sind glaube ich alle bis auf einen, mit diesen unter anderem spekulativen Attacken durch Geldfluss entgegenzuwirken. Wenn jetzt allerdings eine Kryptowährung wie Bitcoin so groß wird, dass diese für eine solche Attacke genutzt werden kann... das liegt ja noch, wenn überhaupt, weit in der Zukunft, aber könnte eine Gefahr darstellen, wie sollte das gestoppt werden? Müsste es da Regelungen geben, das hatte ich überlegt, prozentual eine gewisse Anzahl dieser Währung zu kaufen und der IMF zu übergeben oder sehen Sie da andere Möglichkeiten? #00:35:34-4#

Fiedler: Ich sehe eine große Gefahr in dem Thema Marktmanipulation. Man kann nicht ausschließen, dass diese heute schon stattfindet. Ich persönlich glaube sogar, dass sie schon stattfindet. Es gibt einige große, sogenannte „Wale“ im Markt, die mit sehr großen Volumina traden und, nicht nur bei Bitcoin, sondern auch anderen großen Währungen. #00:36:02-9#

I: Pump and Dump. #00:36:02-9#

Fiedler: [lacht] Genau, Pump and Dump ist das Stichwort. Teilweise machen die Kurse Sprünge nach oben oder nach unten, die völlig irrational erscheinen. Da ist davon auszugehen, dass Diejenigen ihre Marktmacht missbrauchen um bei einem sehr kleinen Order-Buch dort mit Insider-Informationen sehr viel Geld zu verdienen. Das ist auf klassischen Finanzmärkten ganz klar reguliert. Dafür kommt man ins Gefängnis, falls man Derartiges tut. Streng genommen ist mir persönlich kein Gesetz bekannt, dass das bei Kryptowährungen verbietet. Ich gehe davon aus, dass man, wenn man es im Nachgang feststellt, in einem Land wie Deutschland sagt: „Du hättest wissen müssen, dass das verboten ist." Es ist jedoch mindestens eine Grauzone. Da müssen aus meiner Sicht ganz klare Regeln her, die dazu führen, dass jeder weiß, was er tun darf. Außerdem muss eine Verfolgung stattfinden, damit die, die das ausnutzen, auch entsprechend bestraft werden können... und am besten auch bestraft werden um andere abzuschrecken. Das ist ein weiteres Zeichen für dieses sehr frühe Marktstadium des Kryptotradings. #00:37:34-8#

I: Dann sage ich vielen Dank für das Interview! #00:37:40-5#

Anhang 6: Experteninterview Daniel Jeffries

Name	Daniel Jeffries
Aktuelle Institution	Freischaffend
Funktionsbezeichnung/Titel	Freischaffender Autor / Selbstständiger Entwickler
Kontaktdaten	Los Angeles
	cicada@iamcicada.com
Datum des Interviews	05.12.2017
Freigabe	nicht erforderlich

I: At first to put you into context in my bachelor thesis, I would like you to very briefly about a minute describe your career and your current field of activity and the points of contact you have with the topic of Blockchain and Bitcoin. #00:00:23-4#

Jeffries: Sure. I've been in the tech industry for 20 years. I had my own consulting company where I primarily consulted for back office infrastructure and web companies building servers networking and scalable systems. I took an early interest in open source and did a lot of stuff with Linux. After I sold my company, I worked at red hat for eight years which is the biggest linux open source funder in the world. I started getting interest in Bitcoin in 2013. I wrote my first article about Bitcoin in 2014 for Bitcoin magazine. One of the co-founders of the magazine was Vitalik Buterin. I used to chat with him on the writer Skype channel when he was inventing this little technology called Ethereum. I was there when he first put out the original paper and articles on Ethereum and when he was conceiving the concepts of it. I've been involved in for a long time, and my interest only waned for small periods of time after the collapse of Mt. Gox which was particularly annoying but my interest in the technology has never really waivered. #00:01:58-4#

I: Perfect. Thank you for that. To get into the topic easy, I would like you to also very briefly describe what you would see as the central characteristics of Bitcoin and Blockchain. #00:02:15-3#

Jeffries: It's pretty simple. A block chain is a distributed consensus mechanism. It distributes power across the system and it forces only the best decisions or the most important decisions to be agreed upon, whereas in a centrally controlled system, a

small group leads change in the consensus roles. Consensus roles existed long before Blockchain. How much money is in supply in a centralized currency like the US Dollar or the Euro, their central banks set the rule. That is a consensus role on how much money being in circulation. They can change that rule without consulting anybody other than themselves whereas in Blockchain because it is a protocol and math-based, the vast majority of people have got to agree to the change. So it makes changes slower, but it also makes sure that only the most important changes get through. There are some people who describe a block chain is nothing more than series of blocks. I think that that is wrong, in other words it's reducing it absurd. I think that if a central power, a single nation state or single corporation controls a block chain, it is not a block chain, it's a database. And in fact it's slower than the database, so it's useless. Only when the system is controlled by multiple ideologies, it is a block chain. If five banks on a block chain, it is not a block chain, it's a database. But if the depositors, the regulators, the banks, the shareholders all have some type of stake in the block chain and some vested interest in the consensus, then it is a block chain. #00:04:32-5#

I: I would like to start right with another technical question about how safe Bitcoin is to use, I mean the Blockchain hasn't been hacked in seven years, but there are those software wallets which could be compromised like Parity for Ethereum had its bug where like 150 millions have been frozen. How safe do you see Bitcoin and wallets in the use? #00:05:03-4#

Jeffries: I see Corewallets as very safe. I also see it's gonna be necessary for the technology to evolve for the mass to use it because the average person is not technically skilled enough to go through the procedures. I do see the technology developing and becoming easier for the average person to deal with. I also see both the languages and the protocols developing over the next 10-20 years to more sophisticated libraries that are incredibly secure, languages that are incredibly secure that don't have things like risk conditions and buffer overflows, it will be elderly necessary for smart contracts to be in wide use it. Currently like our languages libraries and such and our security protocols are not good enough to deal with them which is why you see the human error creeping in and 1% changes code on GitHub or there's a security in how people have written the contract, and it causes a lot of people to lose money. That's gonna be unacceptable for it to have wider use, so I expect the technology to develop over time. I've often predicted that decentralized exchanges multi signature wallets and things like that would have tremendous screw-ups in the short terms, but in the long term, the language will absolutely become set and stone; there will be few security vulnerabilities, and you'll eventually see smart contracts will

place most types of several contracts and most types of escrow systems and most types of sort of distributions of money sort of trust purchasing houses things of that nature. The languages and the standards will develop through series of best practices and security protocols that will allow average programmers and average people to use them probably through drag and drop interface where they don't actually have to be aware of most of the code running behind it. #00:07:22-4#

I: But smart contracts are still I would say bound to human error. Do you think the more often specific contracts are beeing used the safer it gets when people improve it? #00:07:35-1#

Jeffries: I think over the next 5 to 20 years, we're gonna see tremendous amounts of improvement. We're gonna see new languages that are developed, a set series of secure libraries that have invaded over and over again, and a set of series of best practices. These are not unsolvable problems. They are mathematically provable algorithms. There are systems control fighter jets of missiles or heart monitored devices. There are series of practices that have already developed in those spaces. There will be similar practices that develop when it comes to programmable money because they will have to develop. There's not a single person in their right mind who would currently put their money with a smart contract at this and hope that the language survives for the next 20 years because it won't. However, in 20 years, I suspect that technology will be nearly written in stone and practically unhackable. It doesn't mean that there will never be an issues, but I do feel that after we've suffered a number of... bits of money being locked up or screwed up or putting the wrong thing into GitHub that security practices and languages and such will develop to make it harder and harder to do that. #00:09:15-5#

I: I would skip to another question. We're just talking about mass adoption, how suitable do you see Bitcoin for the mass because people need I would say kind of technical understanding of private keys, what is a public key and how store your funds safely. Do you see a barrier at this difficult usability? #00:09:39-7#

Jeffries: There's a barrier but that barrier will go away. New technologies will be developed at hard banks where local people are able to just work with their friends and family to create a nethub bank. You'll see wallets that are much just trivial to use like chip or hardware wallet or a wristband or necklace or whatever that they have, they'll be biometric controls to it. All those things will get easier and easier for the average human to use overtime. It's certainly a barrier to entry now whether Bitcoin is the

ultimate series or is the ultimate coin for transacting daily value, I don't see it as that. I see money developing into series of different types of medicoins that have certain properties. One is a saver coin the deflationary coin like Bitcoin which is primarily an investment vehicle or place to store and reward savers. A second one would be something that is more ubiquitous and more like a dollar perhaps slight inflationary or slight deflationary over long term that is incredibly stable, and that's the type of thing where you're gonna but sneakers and books from Amazon with. You'll have different types of currencies. I see Rewardcoins as being another useful way for these things to work. if you think about something like a Starbucks card all you can do is buy Starbucks with your coins. If you have a universal reward system that cuts across different types of platforms rewards you just for using or for doing the behavior that the network likes, then those Rewardcoins will become quite valuable as well. I see the crypto started to basically divide up into differen types of coins. I see Bitcoin being the type of coin that is going to be useful on a day-to-day basis, but there are tons of other coins that hold the potential to do that. Some of them will also just be utility coins or platform style coins. Ethereum is essentially a platform style coin and NEO is platform style coin. You'll also see utility coins. There's not real utility for utility coins at this point, but eventually if you have a decentralized internet where you have 10 different providers of a decentralized DNS, 10 different providers of a decentralized identity each with their own coin and Metacoin to swap those coins and consume the value to do an identity transaction or register your DNS change transaction, and there are some methodology or some system that's sort of setting the prices of those in consensus and exchanging the coins in a seamless fashion. On the backend, those utility coins will become essential as well, so you'll have this sort of market network. Energycoins are good example where in New York City, you already have different solar panels and different neighbors roots. There's decentralized exchange that changes the rate and people access Energy with their neighbors without a centralized group that's controlling it. That's a great example of utility coin that will become quite ubiquitous overtime, and you'll see series of meta utility coins that are able to consume the value of those. Bitcoin in itself is not gonna serve all those purposes nor is it needs to. Other coins will serve those purposes, and in addition you're gonna see the rise of probably hundreds of different types of consensus protocols, and within five years you're gonna see coins that are able to make scale pass these little transactions and make the current scale of these look like a joke. #00:13:39-5#

I: I will jump to the next technical question like the use that transactions cannot be reversed. Do you see advantages or disadvantages for that for companies maybe or for private users? #00:13:59-5#

Jeffries: There's advantages and disadvantages. I think we're gonna see both types of transactions. I think that the protocols will develop in such a way that the money might escrow for a period of time. There might also be pools from insurance funds for fraud or scams that people might pay into that might pay them back. You can basically have the same level of fraud protection that you have now and we just work in a different way. Where the money might escrow for a period of time and you might be loaned as a vendor, you might be loaned that money from a pool for a period of time so you wouldn't have to wait you can use it, but at the same time the money is escrowed and at some point in time like if it is considered fraud then you might lose a portion of your stake in the pool etcetera. So there are definitely ways to create the same level of fraud prevention that we already have people will absolutely do it; it's going to happen. There are also advantages to money where you can't roll the transaction. I think Andreas Antonopolus talks a lot about how we've grown up in a modern world in the last 50 years post world war 2 with the series of soft promises, promises that aren't real and that can be reversed at the drop of hat. In many ways, Bitcoin and cryptocurrencies represent a hard promise and that is one cannot be easily reversed or taken back. And there advantage just of both those systems. Some types of promises should not be able to be taken back. Some absolutely should be reversible. We will see both types of systems develop, and we will see certain types of or certain categories of transactions fall into a best practice for which one of those systems to use. #00:16:10-7#

I: For the next question, I would like to really focus on Bitcoin, how stable you review the ecosystem because there are disagreements between the developer teams and then they hard fork. I had the expression with Bitcoin Cash and many others did as well that it was more like the way to maybe generate money they didn't have replay protection and so on and all those political differences. Does it endanger the stability of Bitcoin? #00:16:42-5#

Jeffries: I don't think so. I think that Hard Forks are a necessary response to the fact that Satoshi did not envision building governance. So things like Tesos and Decrad and Dash have envisioned some type of governance protocol, Satoshi did not see a reason for it at that time; it's one of the problems he did not solve. The only way to solve that is to do Darwin in economics and through competition through those Hard Forks. I see that as a way to resolve those political differences. The best ideas will eventually create enough pressure that the primary Bitcoin pass to adopt them. The ones that only have fanatics they' be true believers and they'll really believe that their coin is going to the moon and will replace Bitcoin, and they will be bitterly and sadly

mistaken and that's too bad. That is what we're heading into, we're heading into an era where you can believe any kind of bullshit that you want about economics, but now you're going to suffer. You're going to pay a price for your stupidity. You will have to... you'll get to try any stupid experiment you like and it doesn't mean it's going to work, but you will learn a hard lesson. In fact, other cryptocurrencies a friend of mine started one where the idea you can fork it essentially on chain and everyone can create their own local chance and local rules. The understanding is that the vast majority they're going to be total failures because people creating them are either idiots or they're blind to the true nature of economics, or they have a perceptual belief system that is flat. People believe all kinds of crazy are shit. We can literally be wired to believe anything that we want. Right now, we have people who still believe that the earth is flat and that it's conspiracy. The system is built, I'm talking about the system of the universe, is absolutely built through any idiot to believe whatever they want. Darwin in economics are now going to teach people very hard lessons. #00:19:10-5#

I: That is like a lot of pump and dump going on. So people with I'd say big pockets can profit from that. They're not getting punished. #00:19:19-4#

Jeffries: Correct. Some of those coins will actually be useful with great ideas. And those coins will take off, and some of those ideas will begin to trickle back into Bitcoin and other coins that matter. This is still very experimental age. Don't forget, we're in the cave-man era of cryptocurrencies. We're in the beginning of triple and trade accounting. Understand that every time there's been a revolution in accounting like it's been a dramatic uptake in human civilization in economic complexity. We've only had two of them, single entry accounting during the era of kings and queens where you only did work transactions with your brother, and because if you wipe out that one line it doesn't exist. Via these traders and the 1400 tried to start doing trading with people they didn't know, so they invented the double entry accounting system, so now all of the sudden goods and services are moving all over the word. I have a debit you have credit. We've reached the end of that, triple entry accounting is gonna be a massive boost to mankind however it develops. You cannot have an n-run style fraud with triple entry accounting. Eventually, 500 years from now, they'll come up with a different way to create fraud. You will need quadruple entry accounting or whatever the hell that is. In the double entry system, if I tell you that I've issued a million shares and you have 10%, you really have no way of knowing that, you have to trust me. You'll never gonna get access to my books in a double entry accounting system because it's security violation. In the triple entry accounting, you can look at the third entry and you can say, okay there are a million shares, I have this many that equals 10%, I know for sure. We

are absolutely in a cave-man era. It actually doesn't even matter if Bitcoin goes to zero, there's no question that cryptography and distributed and decentralized currencies, world currencies as well as the Blockchain and other decentralized consensus protocols are absolutely incredible revolutionary breakthrough of massive proportions. #00:21:37-4#

I: I'd like to guide the next question a little bit more to the Hard Forks and to our current time. I think that Hard Forks might cause a confusion for many people say if I'm new to this topic or to this environments, I end up maybe googling Bitcoin end up with Bitcoin Cash, Bitcoin Gold, Bitcoin Diamonds. Do you see that as discouraging to get deeper into the topic of Bitcoin or to actually buy and use it? #00:22:11-7#

Jeffries: In the short term yes, eventually as the sort of fork becomes kind of either more ubiquitous or less. The people who are holding the coins essentially just got free money. I think most people are like this is great. Most of them got I'm just gonna go down this fork or maybe I'll hold it because I really their ideas and there's an opportunity. So in the long run I think it's positive. In the short term, I think it can confusing and you certainly see a series of orchestrated information warfare campaigns and sort psycho punk style tax on Bitcoin like we saw with Bitcoin Cash. So in the short term I think it's confusing, the long term I don't think it will be. #00:22:50-4#

I: So next question will be about something technical, about the transaction times, miners take the transaction with the highest fees, and the lower fees are the longer your transaction takes, if you even can adjust it in your wallet. Do you see the light in that work as a solution to this, or do you view this as a general problem of Bitcoin? #23:01-5#

Jeffries: The lighting network is our solution to it. It will be both good and bad. My sense is it will generally be good. It will result in a number of sort of centralized payment processors, but it's also entirely possible to have distributed/decentralized side change processor as well. So just like we've seen with miners originally, it was very super centralized, and then you see things like Slashpool have come to the fore fund which is totally decentralized mining pool. In the early days, the mining pools didn't pay out as well, they haven't quite figured out the algorithm so slower, but now Slashpool works as well as any other mining tool and it makes sense. It takes time to do things decentralized way. I fully see a number of decentralized side chain systems, and I think it's gonna be very valuable and despite what fake Satoshi Craig Wright says

that it was only meant to scale on chain, I guess he forgot. I think he was of the first inventors if he was actually Satoshi Nakamoto of side chains. So he actually proposed in one of this emails the in timeline cash which was one of the first examples of potentially how you could build an off-chain payment system. So I guess he just forgot that or he's just a faker like everybody guesses or he's changed his mind. The fact is he's a faker. Satoshi absolutely envisioned off-chain settlement processing, his initial solution was actually fraud, but he never actually implemented it in code, he only proposed it as a potential solution and so now people are working it out. Actually you see it as a potential way to scale, it is not the only way to scale, it will need additional types of algorithmic innovations for it to be exactly what we want, but it's definitely our solution. #00:25:33-9#

I: Another question would be also about the miners. What do you see a problem with more and more centralized proof of work, I mean Ethereum is experimenting with proof of stake and we will see how that works. What do you think about less and less mining pools out there? #00:25:58-8#

Jeffries: I see centralized money is a tremendous problem. I see it as absolutely the worst part of the Bitcoin vision. I see it as the biggest flaw in the Bitcoin vision, and I absolutely think that a network that is more resilient, it is more decentralized. Actually, I designed a concept system called *Cicada* that is inspired by other projects. In that, I created a system everyone is both a miner and a wallet, and essentially the money you randomly drafted into the system like you might just have it on your smartphone and you're walking along and you get the call, you do a proof of work or whatever a proof of sake for 10 minutes, and you potentially win some coins. It essentially is more and more distributed and in fact everyone who comes into the system distributes it. Whether that's the correct answer or not, I don't know, but more and more people are coming up with systems that are harder and harder to centralize. To me that's a good thing because centralized systems are already a choke point. You're seeing that in Russia. The Chinese have not attacked their big miners but they will, and Russians are already proposing that the miners are gonna have to register so that they can come after them. You can absolutely bet in the time of war they would show up with guns and take all of their equipment and all of their coins. And essentially you just handed over a bunch of coins to the state. It's pretty hard to hide your electricity footprint if you're running 10,000 Antminers somewhere. I actually think it is a choke point, but I think that many coins are going to solve that problem in the future. #00:27:49-5#

I: So do you think that Bitcoin might implement prove of stake at some point? #00:27:55-7#

Jeffries: I think so. I think proof of stake has got to prove itself to be as unflappable and unhackable as proof of work. When I was working on a similar concept years ago, I came up with an idea of that resembled proof of stake. There was no word for it, there's no name for it. And as I grew up on the white board over six months, I've thought thousand ways to attack it. I just thought god this can never work. I've been mostly wrong. I addressed a lot of those concerns and built workable proof of stake systems. To this day, we can't be 100% sure that they are as flawless as a proof of work. A proof of work is valued because of its other simplicity. It's kinda like an original analog braking a car versus a digital break that we have now. Analog breaking was basically a couple of moving parts, and we developed a way for them to work pretty much flawlessly every single time. Whereas digital breaks introduced a number of vulnerabilities as we saw with kind of the Toyota Prius accelerating sometimes and getting locked, and they had two teams over six months when the law suits started examine the code for the breaks, the first team failed to find the condition, and the second took another six months and they were pretty sure they found it. So it was a terror of inferno of code. I think simplicity is better and proof of stake is still relatively simple, I don't know what the winning protocol is going to be, but these protocols will continue to develop and absolutely if Bitcoin survives, it will eventually likely adopt a different protocol. However, it faces the fact that the miners will stand against it and might not support it, so I actually see alternative coins being the ones that adopt. The only reason Bitcoin would adopt it would be if it is in serious decline at that point. If another coin was rising and pushing it to the side because it had better governance or better consensus protocol more use worked faster, eventually in order to survive it would have to adopt changes. #00:30:39-6#

I: For my next question, I want to go about the definition of Bitcoin. While I researched for my bachelor thesis, a currency should have the criteria of exchange in payment which should be broadly accepted youth of accounts and start of value. Do you see that Bitcoin meets these criteria or do you rather describe Bitcoin as an asset? #00:31:09-2#

Jeffries: I don't know if it meets the criteria currently and I don't know that those criteria are even accurate for it for what the meaning of a money is. Gold is absolutely not an easy medium of transacting in anything. Transacting with gold is a huge pay in the ass. Nobody would argue that it doesn't have a general store value or some level of utility

even if that utility is fear based. I don't feel that it meets all those criteria, but I also don't feel that it needs to. At this point, it is a hybrid asset and that it is kind of like a share economy kind of like gold and kind of mini transactions, but it's not really any or all of those things 100%. It's not great in any one of those, it just can do all of them relatively well. The answer is no it doesn't need all those criteria, but I have to question those criteria are useful. #00:32:25-2#

I: That's also what my bachelor thesis. I would rather call it an asset than a currency like exactly what you say. I want to go to the next question another question about the stability. The system the Blockchain relies on the trust of the users into it like there's no central entity like the central bank or the Federal Reserve. Do you see this as a chance or as a risk or something in between, do you see possibility that this stability can shake? #00:33:05-6#

Jeffries: It can certainly shake. I see it in the long term as more stable than a centralized governance crypto, not currently, but in the long run. A perfect example is your currency in Germany after world war. By no means is a central government and our faith in that government a guarantee of anything. Because that government... this is what I was saying in my articles. Trust is a moving concept, it is not a fixed concept. People mistakenly understand trust as a fixed concept, it is never, it is moving all times. So if a man is married to his wife for 15 years and he never cheats on her he has 15 years of trust, the second that he goes out and sleeps with another woman, all of that trust is burned up overnight and he's no longer trustworthy. If a company was trustworthy for years and suddenly begins doing all kinds of shady shit because they hired the wrong people, then that company has no trust. Venswill is a perfect example of a country there was a thriving economy that was looking to break out of banana republic status into becoming a real power house and got the wrong people in charge and suddenly crashed the economy and people are starving. The same if you look at Germany after world war one, both the fact that they lost the war and then they were also required to pay for the war after being totally broke, and the fact that they were being crushed while essentially the rest of the world was moving, created an absolute witches pentagram that lead to the rise of the Nazis of world war two. It was directly responsible, the economics were directly responsible for it. It's like there's an old saying in China that when the price of rice is high, heaven decrees new rulers. That is true of all kind. Overtime, I see a protocol where everyone has a stake in being valuable even people who disagree from the Russians and United States and Venezuela, all potentially have a stake in Bitcoin being profitable or a decentralized cryptocurrency working. Then I believe that that is more powerful than a single nation stake which

could put in the wrong people. It's less likely that all of the nation states would simultaneously go bed in the world and destroy a truly decentralized currency that is ubiquitous and widely used, then a currency that is backed only by a single nation which can go bed overnight because they elect the wrong people, or they mix the policies, or they have an economic crash that brings the wrong people to power. #00:36:11-7#

I: So in conclusion, the market itself has globally more interest in stability than if a central entity would control it. #00:36:20-1#

Jeffries: Correct. #00:36:27-5#

I: I would go to the next question about the influence of volatility of bitcoin because I have this topic in my bachelor thesis about Bitcoin as a currency. For the volatility would be the question whether it would be economical or whether you see it as economical to use Bitcoin for payments today or in the future because I could have one Bitcoin and say it's 10,000 now and I want to buy a car, but I could wait up in two weeks and it would 15,000 and I would be angry with myself that I didn't save it or didn't attach it. How do you view the volatility goes upwards? #00:37:19-6#

Jeffries: It's not gonna be as volatility in the coming years. It's volatility because of the style of Banana Republic. If you look at any emerging economy in history of man, they are all incredibly evolved. Eventually, any system that is growing is chaotic. Eventually a system achieves equilibrium and the volatility becomes a lot less. This is what we're gonna see with Bitcoin as well. I see the volatility is as a temporary way for speculators and such to make money, but overtime as the utility rises the volatility decreases. #00:37:57-7#

I: Once gold has been taken away from the dollar, I think it was as volatile as Bitcoin is now. Do you think that when it gets stable, it will have greater chance of being used as a currency, or do you think if it's stable it will still be a medium of speculation or a sore value? #00:38:21-5#

Jeffries: I kinda see Bitcoin as being something that's going to be a long term saver coin when it comes to the meta properties and coins. I don't see it as a likelihood that people are gonna be buying their coffee with Bitcoin. It's feasible but I just don't see it being the case, and that's fine it's absolutely fine. Other coins will be able to pick up

that capability and it's perfectly fine to have Bitcoin as an asset that rises in value overtime and rewards people for saving things. Now in the world, we reward people for being as crazy with borrowing money as possible. It rewards people for borrowing as much money as possible and deliberately defaulting, whereas in the past it rewards people for saving their coins in order to buy something off value. I see Bitcoin continuing to have those properties in the long term and that's fine. It doesn't need to be you don't need to be buying coffee with it. #00:39:40-7#

I: Another question would be about the transparency of the systems. So if I'm a company and I have a wallet address set out and nearly everyone can confirm how much has been sent to it, do you see this as a barrier for companies to use Bitcoin or for accepting Bitcoin or users to send Bitcoin if they maybe don't generate a new address every time? #00:40:06-6#

Jeffries: In the long term, it's gonna be able... it will prevent fraud and it will be able to know where their companies have money in the bank instead of guessing. I think people have widely looked at Bitcoin and said my god like you build a track all these transactions, absolutely correct. Alternative coins will have better cash properties and that will be okay, but there's a lot of value actually in being able to know that Sony Corporation has xyz number of dollars in the bank and it's not just reporting falsely to the SCC. I think that companies eventually will have it as a point of pride to be able to show within the distributed ledger that a certain amount of money flowed into it. I think that's gonna become a point of pride for many times. #00:41:09-1#

I: I don't know if I included the following in the lead questions I sent you because it's a new question that I asked myself about loss about Bitcoin. Do you know the IMF which is responsible for stability for currencies like the central bank and the Federal Reserve Bank? #00:41:31-8#

Jeffries: Yes. #00:41:32-5#

I: Okay perfect. The IMF collects money from the states who participate I think it's every state but one and when somebody tries for example a speculative attack, the IMF can come to that with their money. Is Bitcoin or other currencies might rise it does not have any money, so do you use the problem that people could use Bitcoin or another cryptocurrency for false speculative text, and do you see any solution for that problem? #00:42:04-5#

Jeffries: Yeah sure. There's no reason you couldn't continue to have an IMF holding a whole shit kind of Bitcoin or other currency in stall for the same problem. You gotta actually see a number of decentraled tools which would be highly decentralized, but you might see the rise of 5 or 10 different organizations that are similar to the IMF. And in actual reality that's better because they're competing, whereas the IMF in essence is the only body... and by the way, their policies have not always proven to be correct. Some of their policies where they basically said you need really harsh austerity, regardless of the other economic factors has not always proven to be correct. It's directly lead to the collapse of a number of economies. You might see three or four pools of crypto coins that might have different policies and the governments of the world might go to the different ones and they might have to compete in order to have those policies. By the way, that means those economic policies will then play out in the real world. The problem is with all of our economic policies the very few people seem to understand is that all of our economic theories are developed largely on bull shit. They're developed on analog statistics 100 of years ago. So people have these economics is a freaking religion on Austrian Tunisian or whatever. It's like what is it based on, it's based on a bunch of old men who studied a bunch of faulty statistics 100 years ago, what good is that? The fact us understanding of economics is gonna start to play out in real time, and we're going to learn a whole bunch of things about economics now that we didn't understand because we're gonna have real time data real time statistics, and we're gonna have competing ideologies, and that's going to actually be a good thing in the long term because we'll actually learn what works and what doesn't as opposed to just guessing which is essentially what we've done now. #00:44:15-5#

I: Do you think that the states will keep up in time with loss to do this? If for example the IMF has to collect enough Bitcoin to counter speculative attack, it might need to require every state to buy a percentage for it. Do you think this will happen? #00:44:36-3#

Jeffries: We willingly do it. In other words, I think you already see and the Asian countries and such start to build their own kind of counters to the IMF with currencies. Why wouldn't many states simply bond together to form pools of cryptocurrencies and set their own economic policies. I foresee it absolutely happening. I don't actually see it being any different in many respects than it already is. In fact, I actually see it potentially developing as long as we live long enough into even algorithmic ways to stabilize economics, but essentially narrow artificial intelligences where there's not even necessarily people behind it where people nation states and this is too farfetched for the average person to understand today, but in 10 or 20 years when artificial

intelligence is governing a huge amount of the nation or of economics [phone call] Alright, we're coming close to the end here I think. Anything else that sort of really important that you wanna go over? #00:46:52-6#

I: No, that's basically every of my questions. Thank you so much for doing it, it was very interesting. #00:47:02-9#

Anhang 7: Experteninterview Darshini Dalal

Name	Darshini Dalal
Aktuelle Institution	Deloitte Consulting LLP
Funktionsbezeichnung/Titel	Technology Strategist
Kontaktdaten	200 Berkley Street
	02116 Boston
	ddalal@deloitte.com
Datum des Interviews	05.12.2017
Freigabe	nicht erforderlich

I: Thank you for your time. Please describe your career briefly, as well as your points of contact with this topic. #00:00:20-8#

Dalal: I work for Deloitte Consulting LLP in Boston as the leader of the „Blockchain Lab“, where we evaluate nationally and globally how upcoming related technologies will develop and provide consultancy services to other companies on how to implement this technology into their business. This has been my current field for three years now and I have come in contact with Bitcoin nearly every day. #00:00:44-9#

I: Ok, thank you very much. I would like to jump right into the second question. I would like you to explain the central characteristics and key aspects of bitcoin and its blockchain. #00:01:08-9#

Dalal: Why are you asking me what these characteristics are? Do you know them yourself or do I need to explain them? #00:01:24-6#

I: Those lead questions are the question go through to one where I would like to ask you to assess the chances and risks Bitcoin offers as a medium of exchange, which resembles my scientific question. I used that easy question to start the interview. I do know the answer to it, but I used it as a conversation starter for the interview. But we can surely jump to the third question. #00:01:58-1#

Dalal: No, that is ok. In my opinion Bitcoin’s biggest advantage is that the value of the system is not held by anyone, except the person holding the keys to his transaction in

the ledger themselves. There are no intermediaries, there is the finality of bitcoin and the cap associated with it. So, I think that those are the core functions of the coin. There are, of course, other uses - cases of Bitcoin as equity. Rather than using a physical currency you can use bitcoin as a digital currency. #00:03:40-6#

I: Ok, thank you. Let´s get right to the next question. The Blockchain has not been hacked in seven years, but wallets can be compromised. How safe do you view the use of bitcoin? #00:04:20-1#

Dalal: In my opinion, if you are smart and know about wallets and how to use them, I see them as safe. There are a lot of people out there who are buying Bitcoin every day and know how to use them. But you are right. Wallets, especially software ones, can technically be hacked or include bugs. Therefore one has to be careful. I think people need to be educated about what a wallet really is and how to store your funds correctly; how to use a public key, how to store a private key, and so on. But I think besides that Bitcoin is rather safe to use and can be accepted by many merchants, not to mention its economic aspect, its transaction fees. #00:05:23-3#

I: Thank you. That fits with another question on my list. How suitable do you view Bitcoin as wallet for the masses? Like we just mentioned, the user needs to have a technical understanding about the topic. Do you see a barrier in this difficult usability? #00:05:51-1#

Dalal: Somewhat. I think it depends on the technical understanding of the person. But I believe that people can learn, though you are right. A big barrier exists. #00:06:10-1#

I: Thank you. Transactions cannot be reversed. Do you see any disadvantages or advantages for private users or companies here? #00:06:39-6#

Dalal: I don´t know if I would call this either a disadvantage or an advantage. I think this is more of a feature that people will have to adapt to. When we are talking about not being able to reverse the transaction, we are talking about a human error in that it got send to the wrong address. People in companies will have to be schooled to learn the skills and I believe this will work fine. We also have to look at what the use of it is beyond transactions. But with smart contracts, these required skills are surely more and more specific. On the private sector side, I don´t know whether it has the potential to achieve mass adoption. #00:07:53-8#

I: Ok, thank you. Another question would be about the stability of the system. There are political differences between the developers, like with Bitcoin Cash and Bitcoin Core. Hard-forks happen. Do you believe that the ecosystem as a whole is stable? #00:08:31-1#

Dalal: I would like to say „It´s not a matter of stability. It is a governance issue." When you have a public blockchain, such as bitcoin, it is about the number of people who control the development – like with bitcoin core or bitcoin cash. It is a very small group, yet bitcoin has proven to be very stable. The forks offer a more or less democratic option to go against a settled opinion. #00:09:27-1#

I: Thank you. Another question is about the possible confusion of hard-forks. Do you see the many different versions as a discouragement for people who are new to this topic? #00:09:44-6#

Dalal: I think that the better people understand the technology and experiment with it, the more they will get used to this topic. With smartphones taking over more and more tasks in our everyday lives, so bitcoin could also someday be mass adoptable without people having to know a lot about their tech. It could just... work. #00:09:587#

I: Thank you. My next question is about the transaction fees. Those are very high at the moment. Do you see a problem here or maybe a possible solution? #00:10:07-8#

Dalal: I think, yes. There is a problem, but in my opinion Bitcoin is not a network made for mass adoption in terms of a payment perspective. I think it should be taken into consideration to introduce a Proof-of-Stake. #00:10:57:1#

I: Thank you. As a further question I would like to ask whether you see a problem in the more and more centralized Proof-of-Work ecosystem? #00:11:11-9#

Dalal: I don´t think that I really see a problem there, but rather in the concept itself. It is more and more vulnerable to a 51% attack with the size of the mining pools increasing and the number decreasing. Like I said, Proof-of-Stake might be a solution here, but this has to be figured out by the developers. #00:12:11-6#

I: Ok, then I will head to my next question. I want to define Bitcoin and a currency has three central aspects: a medium of exchange and payment, a unit of account

and a storage of value. Do you think that bitcoin fulfils these criteria? #00:12:50-1#

Dalal: In my opinion the coin is being defined as a cryptocurrency by the media and most of its users. I don´t think that there should be a question about whether this is a currency or not. It should be about whether bitcoin as a crytocurrency may or may not have the potential to fulfil what fiat money does. So, whether bitcoin is able to fulfil the everyday life purposes that fiat money is used for. In my opinion it does not do that at the moment. #00:13:09-5#

I: Thank you. Regarding the volatility of bitcoin, do you reflect on this being economical? Or do you see a barrier here to use it as a currency? #00:13:126#

Dalal: This is a question of supply and demand. Eventually the volatility will go down because the market capitalization will increase. Right now it is not economical, that is true, but in a few years... it has the potential to be economical. #00:13:45-8#

I: My next question touches the topic of transaction fees. Miners take the transactions with the highest fees and the lower the fees, the longer the transaction times. What is your opinion on that? #00:14:05-2#

Dalal: Yes, this is a problem. But maybe only a temporary one as many alternatives are being developed at the moment. Take the Lightning-Network. The market demand solves the problems. Right now, it makes bitcoin as a currency uneconomical. But in the future it could work. #00:14:16-7#

I: Thank you. Another question I have is about the adoption and acceptance of Bitcoin as a payment method. Right now, Microsoft and other big companies are starting to offer it as a payment method, even though the fees are high. Do you reflect on this as an increase in acceptance or rather a method of marketing? #00:14:25-5#

Dalal: I see a potential here. Bitcoin is increasingly accepted and it is here to stay. Like I said, I see the problem with the fees as more of temporary one. #00:14:47-9#

I: Ok, thank you. That is all the questions for now. Thank you very much! #00:15:01-2#

Anhang 8: Experteninterview Prof. Dr. Bernd Thomas Ramb

Name	Prof. Dr. Bernd Thomas Ramb
Aktuelle Institution	Aufsichtsrat der Gesellschaft für Wirtschaftssysteme Kassel / Emerit
Funktionsbezeichnung/Titel	Aufsichtsrat / Emeritierter, promovierter und habilitierter Professor (Wirtschaftspolitik, Geldtheorie, Geldpolitik und Europäische Politik)
Kontaktdaten	bernd@ramb.de
Datum des Interviews	05.12.2017
Freigabe	nicht erforderlich

I: Zu Anfang möchte ich Sie bitten, Ihren Werdegang und Ihre Tätigkeit und die Berührungspunkte mit dem Thema einmal aufzuzählen. #00:01:39-4#

Ramb: Alles klar. Also ich bin von Haus aus, eigentlich Mathematiker. Habe ein Studium in der Mathematik mit Nebenfächern Physik- und Betriebswirtschaftslehre absolviert. Als Diplommathematiker bin ich dann zu den Volkswirten gewechselt, habe in Wirtschaftswissenschaften promoviert und anschließend habilitiert im Fach Volkswirtschaftslehre. Meine Schwerpunkte, also Forschungsschwerpunkte sind damals wie heute die allgemeine Wirtschaftspolitik, die Geldtheorie und Geldpolitik und die ökonomische Verhaltenstheorie. Da bin ich auch heute als Emeritus noch tätig und forsche so ein bisschen, sozusagen als Privatgelehrter. Der Berührungspunkt mit dem Bitcoin, der Sie ja interessiert, der ergab sich eigentlich aus meiner Analyse der Falschtricks der Eurowährung und im Züge dieser Analyse hat sich auch schnell für mich ergeben, dass zwangsläufig eine Suche entstehen wird nach einer Ersatzwährung, zu dem Euro eine Parallelwährung. Und da habe ich dann vor etwa 7-8 Jahren, also seit dem Beginn des Bitcoins den Bitcoin entdeckt und auch seine Vorzüge entdeckt. Seitdem befasse ich mich so auch mit der Entwicklung des Bitcoins. #00:03:06-5#

I: Alles klar. Vielen Dank. Dann würde ich sagen, steigen wir direkt in die erste richtige Frage ein. Es eine ziemlich einfache Frage, und zwar, was für Sie quasi zentrale Eigenschaften von Bitcoin und dessen Blockchain ausmachen? #00:03:25-5#

Ramb: Also die zentrale Eigenschaft des Bitcoins ist zweifellos seine Nichtstaatlichkeit und seine Begrenztheit in der Emission. Dadurch unterscheidet er sich fundamental von den staatlichen Fiatwährungen, die ja beliebig erweiterbar sind. Blockchain selbst ist für den Bitcoin, für die Interaktion, also für den Handel, für den Austausch von Bitcoins ein zentrales Element, weil auch der Handel des Bitcoins außerhalb der staatlichen Aufsicht passiert. #00:04:00-1#

I: Okay. Danke. Dann würde ich sagen, gehen wir auf die Nutzung ein, und zwar wäre meine erste Frage dabei, dass Zahlungen ja in der Blockchain nicht rückgängig gemacht werden können. Sehen Sie dabei Vor- und Nachteile für Unternehmen oder auch für private Nutzer? #00:04:16-9#

Ramb: Also dieses nicht Rückkehrbar- oder nicht Umkehrbar-Machen von Transaktionen in Bitcoins hat selbstverständlich Vor- und Nachteile. Der Nachteil ist, hat man sich vertan in der Adresse, ist das Geld futsch. Auf der anderen Seite, jeder Nutzer des Bitcoins kennt diese Spielregel und muss sich entsprechend darauf einstellen und wenn er sich vertut, hat er sich vertan. Dann ist das Geld halt weg, aber ohne dieses Risiko gibt es kein Bitcoin. #00:04:50-9#

I: Das stimmt. Dann würde meine nächste Frage sich an die sehr langen Transaktionszeiten richten. Die richten sich ja fast gegen den Grundgedanken vom dezentralen und eher gering gebührenden System. Die Miner nehmen die Transaktionen mit den höchsten Fees. Je weniger Transaktionsgebühren, desto länger dauert das. Sehen Sie da ein Problem? #00:05:19-5#

Ramb: Mit der Dauer der Transaktion? #00:05:21-8#

I: Genau, mit den Kosten. #00:05:23#

Ramb: Ja gut. Diese Kosten und Dauer der Transaktion sind auch etwas was also zum System gehört. Wem das zu lange dauert oder wer da Nachteile drinnen sieht oder bzw. wenn Bitcoinhalter da der Auffassung sind, sie müssten also diese Nachteile in irgendeiner Form überwinden, dann werden sich entsprechend den fundamentalen ökonomischen Gesetzen Institutionen herausbilden, die also diese Geschichte umgehen beispielsweise. Das ist vielleicht vergleichbar mit dem Bankensystem in Bezug auf die Zentralbank. Wenn Sie also mal den Bitcoin als Zentralbank verstehen, denen sich auch in der normalen Währung dann Subsysteme/Bankensysteme, die diese Transaktionen managen und entsprechend halt mit kürzeren Laufzeiten

Transaktionen in Bitcoin vollziehen, die sie aber dann intern später verrechnen, sozusagen an den Nutzer einen Zwischenkredit abgeben. Wenn Sie so wollen, ähnlich wie dem Target-Kredit beim Euro. Also es werden sich automatisch dann entsprechende Subsysteme bilden, weil dann Anbieter von diesen Subsystemen erkennen: „Hier ist ein Markt. Hier möchte jemand eine schnellere Transaktion. Ich biete ihm das an, ich biete ihm eine schnellere Transaktion an. Dafür musst du eine kleine Gebühr bezahlen und ich übernehme dafür das Risiko, dass diese Beträge dann erst später wandern.“ Also da sehe ich im Prinzip kein Problem. Wenn das unangenehmer werden würde für das Bitcoinsystem, würden sich automatisch dann Untersysteme bilden, die das lösen. #00:07:08-4#

I: Also würden Sie auch sagen, dass quasi auf der technischen Seite Bitcoin theoretisch auch vielleicht sogar etwas wirtschaftlich als Zahlungsmittel benutzt werden kann? #00:07:19-5#

Ramb: Ja, auf jeden Fall. Also momentan ist natürlich die Situation so eine besondere, weil der Kurs am Explodieren ist, aber auf die Dauer wird sich der Bitcoin also auch als 08 /15 Zahlungssystemen auch für kleinere Transaktionen, wenn Sie was weiß ich, in New York bei Starbucks ein Becher Kaffee bezahlen wollen, wird sich das immer weiter durchsetzen, weil diese Schnelligkeit der Übertragung durch Subsysteme aufgefangen werden kann. Aber wie gesagt, ich sehe die momentane Funktion des Bitcoins weniger als Tauschmittel als mehr als Wertaufbewahrungsmittel oder wenn Sie so wollen, für bestimmte Leute als Stimulationsobjekt. #00:08:07-6#

I: Okay. Danke. Dann würde ich auch noch auf die Nutzbarkeit eingehen, und zwar gibt es ja im Bitcoin-Ökosystem oft auch Uneinigkeiten, es gibt Hard Forks, wo sich das letzte Mal das Bitcoin Cash Team abgespalten hat. Da gab es auch ein paar Auseinandersetzungen, also als wie stabil schätzen Sie das Ökosystem von Bitcoin überhaupt ein? #00:08:32-5#

Ramb: Das ist alles etwas, was in der Übertragung des zentralen Bitcoinsystems auf das unmittelbare Marktgeschehen oder auf die unmittelbare Nutzung abspielt. Natürlich, das ist das, was ich unter Subsystemen auch verstehe. Es werden sich also mit Sicherheit Subsysteme bilden, weil sie sozusagen vom Markt gewünscht sind oder von Benutzern gewünscht sind. Dass die untereinander auch konkurrieren und sich irgendwie in die Quere kommen, halte ich nicht für einen Nachteil. Also nach meinem Verständnis geht das alles in Richtung Konkurrenzwährung bei diesen Subsystemen

und das ist ja gerade im Hayekschen Sinne die ideale Konstellation, um dieses monopolistische Währungssystem der Staaten zu unterlaufen. #00:09:23-8#

I: Ja genau. Und sehen Sie dann, das ist natürlich dann auch eine Sache, die sich auf lange Zeit zeigen muss, in diesen Hard Forks vielleicht Verwirrung, wenn ich jetzt als Nutzer wirklich auch am Bitcoin-Ökosystem teilhaben möchte und google jetzt zum Beispiel Bitcoin und da stelle ich fest, da sind quasi Versionen wie Bitcoin Cash, Bitcoin Goals, Bitcoin Diamonds letztens auch noch herausgekommen. Ist das so eine Barriere? #00:09:44-5#

Ramb: Bitcoin online, das Geben und eine ganze Menge anderer Derivate aus diesem Bitcoinsystem und da wird sich zeigen, was dem Markt überlebt und was dem Markt nicht überlebt. Da wird das auch den ein oder anderen Kollaps geben, also das habe auch schon gehabt aus dem Bitcoinsystem selbst, wo Diebstahl vorkam im großen Umfang bei den Mt. Gox Zusammenbruch. Das sind alles, ich würde es mal flapsig ausdrücken – Kinderkrankheiten, die man einfach hat. Ich würde gleich einmal gerne in den USA mit der Gründung der Staaten fortfahren. Da gab es auch ein halbes Dutzend Währungen, ein halbes Dutzend Dollarvarianten, die zum großen Teil zusammengebrochen sind, die zum großen Teil einzelnen Regionalbanken zugewiesen waren, die dann ausgeraubt wurden oder was weiß ich auch immer. Auf die Dauer hat sich das dann in, wenn Sie so wollen, darwinistischer oder ich sage dann auch immer im Sinne der ökonomischen Effizienz herausgestellt, ein starkes System, und diese Situation werden wir im Bitcoin auch haben. Es gibt die Derivate, es gibt die Subsysteme, die miteinander konkurrieren. Die schlechten Werte werden vom Markt verschwinden. Die Guten werden überleben, aber überleben werden auf jeden Fall einige Systeme. #00:11:14-3#

I: Okay. Wir wären jetzt beim Thema Markt. Da würde ich zu einer Frage zurückgreifen, und zwar wie die Währung oder die Stabilität der Währung zu definieren ist, beruht ja auf dem Vertrauen der Nutzer in das System, also das System selbst ist ja nicht durch Versprechen des Staates gedeckt. Wie ordnen Sie das in Bezug auf die Stabilität ein, dass der Markt quasi Interesse daran hat , vielleicht auch nicht Bitcoin stabil zu halten und keine zentrale Entität dahintersteht? #00:11:42-4#

Ramb: Ja, zunächst einmal ist ja das interessant: Bitcoin ist eine suprastaatliche Währung, also auch über Staaten hinweg eine internationale Währung und da wird es natürlich immer den Vergleich mit dem aktuellen Staat geben, indem sich die

Bitcoinnachfrage befindet. Ist er in einem Staat, dessen zentrale staatliche Währung sehr angreifbar ist, sehr inflationsträchtig ist und sehr ungewiss ist, sehr instabil ist und dann wechselt er automatisch... versucht automatisch zu Bitcoin überzuwechseln, weil das für ihn eine relativ größere Stabilität ist. Der Bitcoin hat auch eine gewisse Instabilität, vollkommen klar, aber das ist immer ein Vergleich, ein interner Vergleich mit dem konkreten Staat, in dem man sich befindet und dessen Versprechen einer stabilen Währung, die nun wirklich nicht immer sehr fundamental sind. Also selbst im Eurosystem haben wir im Grunde genommen auch einen Verfall der Währung, einen impliziten Verfall der Währung , und deswegen werden auch Nutzer, die im Eurosystem leben, verstärkt auf den Bitcoin überwechseln. Also das ist ein Abwägungsfall/eine Vergleichsfrage, die Chancen und Risiken des Bitcoins werden verglichen mit den Chancen und Risiken der entsprechenden staatlichen Währung. #00:13:10-7#

I: Okay. Wenn wir schon bei dem Thema Volatilität sind, würde ich noch einmal auf die Wirtschaftlichkeit zu sprechen kommen: Für wie wirtschaftlich halten Sie die Nutzung von Bitcoin? Ich meine, es ist sehr volatil, aber auch sehr volatil nach oben. Es könnte auch eine Hemmschwelle sein, dass Leute sagen „Oh, mein Bitcoin ist heute 12.000 wert und nicht, dass er in einer Woche 13.000 wert ist und ich ein Produkt bestellt habe und quasi, wenn es da ist, ist es eigentlich schon... hätte ich meine Bitcoin gehalten, hätten diese eigentlich schon 10%/20% zugenommen“. #00:13:42-3#

Ramb: Ja also, zunächst einmal zeigt das, dass der Bitcoin momentan weniger stark ist als eine Handelswährung, eben gerade, weil sie also diese Preisungewissheit haben. Das hätten Sie auch, wenn Sie/wenn wir so alle erleben und haben eine Überinflation oder jetzt auch vergleichbar mit der Türkei, mit einer so großen Inflation. Da wird die Preisgestaltung natürlich schwieriger, weil beim Bitcoin ist es so: Sie haben prinzipiell ein deflationäres System und kein inflationäres System. D.h. also, ein Computer, den Sie vor fünf Jahren noch mit 10 Bitcoins bezahlt haben, der würde heute nur noch ein Zehntel Bitcoin kosten und dann ärgert man sich natürlich, dass man vor fünf Jahren da diese 10 Bitcoins hergegeben hat, also 100.000 € für einen Computer bezahlt hat. Das macht die Nutzer vorsichtig und deswegen sehen wir Bitcoin eher als Wertaufbewahrungsmittel, insbesondere halt vor dem Hintergrund: Bitcoin ist zwar volatil. Der Kurs bricht auch mal um 10%/20% ein, aber der langfristige Trend ist ganz eindeutig. Der langfristige Trend ist explodierend. Also es würde mich nicht wundern, wenn innerhalb der nächsten 3-5 Jahre der Bitcoinkurs bei 100.000 € liegen würde. Das halte ich für eine mittlere Wahrscheinlichkeit. Das sagt eben: Ich

nehme also heute den Bitcoin nicht als Handelswährung, sondern als Wertaufbewahrungsmittel und wer mutig genug ist, kann es auch als Spekulationsobjekt nehmen und kann Bitcoins zum jetzigen Kurs von 2000 € dazu kaufen in der Erwartung, dass sich der Kurs dann innerhalb von fünf Jahren verzehnfacht. #00:15:44-7#

I: Okay. Vielen Dank. Da würde ich noch eine Frage, die ich ausgelassen hatte, eine technische Frage noch einmal angehen, und zwar ist das Proof of Work System durch die Miningpools usw. immer zentralisierter und auch eigentlich gefährdet durch Absprachen. Wie stufen Sie das ein? #00:16:01-8#

Ramb: Ja, dieses Proof of Work System ist ja auch etwas, was dazu führt, dass die Transaktionszeiten immer länger werden und immer komplizierter werden und das alles... ja, was heißt zentralisiert? Also, es ist alles ein Peer-to-Peer System. Es gibt ein gewisses Restrisiko, aber wie gesagt, das sind Dinge, die dieses Bitcoinsystem zunächst einmal schwerfälliger machen, aber auf Dauer gelöst werden können durch ein Clearingssystem von Bildsituationen, die sagen „Ich übernehme diese Probleme, die daraus entstehen und Du kannst dafür von mir eine Subwährung in Bitcoins bekommen und damit auch handeln, wenn es der Tauschpartner nimmt oder auch als Spekulationsobjekt kauft“. Bei Spekulationsobjekten spielt diese Transaktionszeit oder diese Voluminösität der Datenmenge eine geringere Rolle, weil Sie machen ja keinen Sekundenhandel mit Bitcoins, sondern wenn, spekulieren Sie auf einen mittelfristigen Zeitraum. Wie gesagt, diese ganzen Probleme, die in diesem Bitcoin... zentralen Bitcoinsystem entstehen - Transaktionsverhalten, Daten, Volumen usw. und so fort. Die lassen sich entsprechend auffangen durch Anbieter von Subsystemen, die sagen „Ich übernehme diese Probleme und Du kannst dafür kurzfristiger handeln und musst halt dann dafür ein paar tausende von Bitcoins an Gebühren bezahlen“. #00:17:57-8#

I: Okay. Danke. Dann würde ich noch einmal auf die Definition eingehen, und zwar geht es bei mir darum, ob ich jetzt Bitcoin überhaupt als Währung definiere. Laut der Literatur, die ich dazu zu Rate gezogen habe, muss eine Währung eigentlich ein Tausch- und Zahlungsmittel sein, was auch breit akzeptiert ist, Recheneinheit und Wertspeicherung. Sehen Sie das bei Bitcoin als gegeben an, würden Sie Bitcoin als Währung einordnen, definitorisch? #00:18:22-8#

Ramb: Ja, mehr und mehr. Also es ist so, dass auch klassische Währungen, nationale Währungen nicht immer 100% diese Eigenschaften erfüllen. Und wenn Sie gerade mal den Euro nehmen, das ist kein Wertaufbewahrungsmittel mehr, das Sie für die Rente

zurücklegen können. Der ist ja nicht mehr so wert. Also insofern ist der Euro auch keine Währung, wenn man das auch also wirklich sehr penibel nimmt. Also man muss es wirklich graduell sehen und das Ausmaß, wo die staatlichen Währungen ihre Eigenschaften anteilig verlieren als Währung und nicht mehr Währung sind oder weniger Währung sind, als man sich das wünschen würde. Dann springt in diese Lücke der Bitcoin rein, also sprich, der Bitcoin wird immer stärker Währung und das sehen Sie auch oder kann man auch daran sehen, dass die Staaten immer interessierter sind an den Bitcoins, wobei also diese Bestrebungen Bitcoins zu verbieten sind lächerlich. Da machen sich auch Nobelpreisträger offensichtlich lächerlich, wenn sie das fordern. Sie können das nicht verbieten. Das ist also ein System, das da ist und selbst wenn man irgendwie versucht das im Internet herauszufinden, wenn sich im Internet Subsysteme finden, das sieht man ja auch so ein bisschen in dem berühmt-berüchtigten Darknet. Nein, also diese Staaten sind auf der anderen Seite natürlich begierig an diesem Bitcoinsystem, von diesem Bitcoinsystem zu profitieren, also dass das auch steuerlich relevant einzustufen ist und dazu müssen wir es offiziell akzeptieren. D.h. also, je mehr der Staat sieht „Aha. Ich kann an diesem Bitcoinsystem verdienen“, umso eher wird er bereit sein zu sagen „Okay ich akzeptiere das Bitcoinsystem als Währung, aber Ihr müsst beispielsweise bei jeder Transaktion eine Transaktionssteuer an den Staat entrichten oder Ihr müsst, wenn Ihr ein Spekulationsgewinn macht, einen entsprechenden Spekulationsgewinn versteuern als Einkommen“. Also da kann man auf die Gierigkeit des Staates vertrauen, dass damit der Bitcoin immer mehr auch offiziell als Währung anerkannt wird. #00:20:42-5#

I: Okay. Danke. Dann würde ich mit meiner nächste Frage auch nochmal auf die Akzeptanz und die Massentauglichkeit eingehen. Als wie massentauglich würden Sie die Nutzung von Bitcoin einstufen? Also der Nutzer braucht ja, würde ich jetzt mal behaupten, schon ein geringes technisches Verständnis, um zu wissen... man muss sich ja mit Private und Public Keys auseinandersetzen, um zu verstehen, wie man seine Bitcoins sichert und wie man Transaktionen durchführt. Wie stufen Sie das ein, die Massentauglichkeit von Bitcoin? #00:21:13-8#

Ramb: Ja, die wird so zunehmen wie die Attraktivität des Bitcoins zunimmt. Darauf wieder mal ein Vergleich: Es gab früher den, wie hieß es bei den Aktien, den Milchmädchenboom oder so/irgendwie so. Da hat man das Bild genommen, dass in dem Moment, wo Spekulationen der Aktien profitabel wurden, dass mehr und mehr Leute, die eigentlich sonst nichts mit Aktien zu tun hatten, sich plötzlich in Aktien

involvierten und das hat damals halt zu dem bösen Effekt geführt, dass dann also die Milchmädchen da eingestiegen sind in den Aktienhandel als der Aktienkurs hoch war. Später ist dann der Aktienkurs zusammengebrochen und die armen Mädels, das ist halt jetzt nicht nur auf Frauen bezogen, sondern auch Männer sind betroffen, dann ihre ganzen Ersparnisse verloren haben. Also, je attraktiver der Bitcoin wird, je mehr öffentlich diskutiert wird, umso mehr Leute werden auch versuchen da einzusteigen und da können wir eigentlich nur hoffen, dass dann dem Bitcoin nicht das passiert, was damals den Aktienkursen passiert ist kurz vor dem großen Crash, das ich aber auch nicht sehe, sondern ich wollte die Parallele ziehen, dass man sagt, also... irgendwann wird dann auch der Otto Normalverbraucher hellhörig und wird sagen „Oh Moment. Das ist doch ein System. Kann ich das nicht für mich nutzen?“ Und wenn das zu kompliziert ist, wird das auch wieder Subsysteme und Anbieter geben, die das mundgerecht servieren bis hin zu dieser Überlegung, die es einmal gab, Bitcoin-Münzen prägen und auszugeben und dann hätten die wieder etwas Handfestes in der Hand und könnten damit operieren. Also lange Rede kurzer Sinn: Das Ding wird massentauglicher, je attraktiver es wird. #00:23:16-2#

I: Okay. Danke. Ich habe noch eine weitere Frage, die mir jetzt im Interview noch eingefallen ist. Ich glaube, die ist nicht im Leitfragebogen drinnen, und zwar wie krisenfest Sie eigentlich Bitcoin einstufen? Gold erzeugt ja quasi Kaufkraft. Wie würden Sie das bei Bitcoin einstufen in Zeiten der Krise? Die kann der Staat wahrscheinlich eher schlecht einziehen. #00:23:41-3#

Ramb: Na ja. Das ist im Zeichen der Krisen... dachte einfach mal... ich hoffe Sie kommen auch auf Ihre Frage mit dem IMF, mit der Zentralbank... oder kommen Sie da auch nur zum Sprechen? #00:23:56-6#

I: Darauf würde ich dann auch noch zu sprechen kommen, also wir können es in einem ansprechen. #00:23:58-1#

Ramb: Okay. Alles klar. Ne, aber es geht darum, was ist krisenfest? Wo brauche ich Unterstützung des Staates oder nicht? Also zunächst einmal absolut krisenfest ist auch kein Gold. Das können Sie vergraben und dann vergessen, wo Sie es vergraben haben. Das kann gestohlen werden von Einbrechern. Das ist wie gesagt beim Bitcoinsystem auch alles drin, also es ist nicht absolut krisenfest. Wie gesagt, es gab darauf schon Bitcoindiebstahl im großen Umfang. Das wird man nie vollständig ausschließen können, das so etwas passiert. Da muss jeder für sich entscheiden, ist das in einer Krise für mich ein Rettungsanker oder nicht. Wenn Sie sehen, wie stark

der Bitcoinkurs steigt, wenn große Staaten oder größere Staaten in eine Währungskrise geraten, ein bisschen so arabische Staaten, die plötzlich sagen „Also ich kann mir nicht immer ewig alles in Dollar und Euro halten und selbst der Yen ist nicht Fluchtwährung genug oder der [unverständlich]“, dann flüchten die in dem Bitcoin als Krisenwährung. Ob der Bitcoin dann diese Krise besser übersteht als andere - das ist ein offenes System. Ich würde auch niemanden raten, also alles auf den Bitcoin zu setzen. Also auch da ist es so, dass eine Diversifizierung der Risikovorsorge immer der beste Rat ist. #00:25:37-8#

I: Okay. Danke. Jetzt würde ich auch gleich nochmal auf die IWF zu sprechen kommen, die ja auch für die Wertstabilität zuständig ist. Ich würde sagen, ich bin ein bisschen drinnen in dem Marktthema und handel da ein bisschen und man könnte davon ausgehen, dass öfter mal Marktmanipulation stattfindet oder es jedenfalls Anzeichen dafür gibt, dass sie stattfindet, aktuell schon und weil Bitcoin größer wird, könnte man damit ja auch spekulative Attacken auf Fiatwährungen ausführen. Wie schätzen Sie das ein, dass die IWF da eigentlich noch kein Vorrat an Bitcoins theoretisch hat? #00:26:15-6#

Ramb: Ja, also zunächst einmal der Internationale Währungsfond ist für mich nicht in erster Linie eine Institution, die die Wertstabilität schützen soll, sondern das ist für mich eher eine Ist-Situation, die die Staatsstabilität schützen soll, indem sie also den Staaten die Möglichkeiten gibt, Kredite zu Kondition zu bekommen, die sie eigentlich nicht verdient hätten. Inwieweit Kursverhältnisse durch die Politik des Internationalen Währungsfonds hier auch durch einzelne Zentralbanken nicht gesteuert werden können, ist uns mit fraglich. Also auch in Zeiten, wo es den Bitcoin noch nicht gab, gab es ja Versuche von Zentralbanken etwas in Zeiten vor der Eurowährung die Kurse zu stabilisieren zwischen DM und Fond oder DM und britischen Pfund. Das war schon im damaligen Zeiten, also vor 50 Jahren, 40/50 Jahren waren das Unterfangen, die allenfalls nur kurzfristig funktionierten, wenn man das über Marktinterventionen gemacht hat. Wenn man den Kurs fixiert hat, dann war das eine andere Geschichte, aber dann gab es andere Reflexionen. Der Bitcoin eignet sich für solche Manipulationen eigentlich sehr wenig, also zunächst einmal müssen die Zentralbanken bzw. der Währungsfond eine Menge von Bitcoins einsammeln. Ich will nicht sagen, dass das möglicherweise insgeheim schon passieren könnte oder würde. Also es gibt durchaus Verdachtsmomente, wo Staaten einfallen „Währungsreserven“ in Bitcoins anzulegen, aber wenn sie das zur Kursstabilisierung von Bitcoins nutzen wollten, dann muss man zumindest sagen, bis jetzt haben sie es weder versucht noch geschafft. Kann durchaus sein, aber ich bezweifle ob das möglich ist, vor allen Dingen dauerhaft

möglich ist. Also der Bitcoin wird sich nach meiner Einschätzung in der Endphase der Ausgabe der Bitcoins zunächst einmal auf ein gewisses Wertniveau einpendeln und dann dieses langsam verändern, je nach Zusammenbruch der eigentlichen Nationalwährung. #00:28:51-7#

I: Okay. Danke. Dann würde ich noch einmal meine letzte Frage ... ja Regulierungsmaßnahmen für Bitcoin jetzt vielleicht im deutschen Raum oder im EU Raum eingehen. Als wie reguliert würden Sie die Nutzung quasi von Bitcoin einstufen? Also laut Steuergesetz habe ich das von Interviewpartnern erfahren, müssen Wertgewinne natürlich erfasst werden in der Steuererklärung oder je nachdem, wo man sie hält. Sehen Sie noch mehr Maßnahmen kommen vonseiten des Staates? #00:29:23-4#

Ramb: Ja, das ist auch eine Frage des Nachweises. Inwieweit können wir also Transaktionen in Bitcoin nachweisen. Wenn Sie natürlich eine offizielle Rechnungsstellung haben von einem Unternehmen, was sagt „Okay. Ich schicke dir jetzt ein Notebook und zahle jetzt dafür so und so viel, hunderte Bitcoins“, dann haben Sie natürlich einen Beleg und das Unternehmen, das also dieses Notebook zu diesen Konditionen verkauft hat, wird das auch vorlegen oder im Rahmen einer Betriebsprüfung offenkundig machen müssen. Also da haben Sie einen gewissen Zugriff des Staates und da könnte man sagen „Ja, okay. Da ist also jetzt Mehrwertsteuer fällig geworden in einer Höhe von so vielen Bitcoins“, dann müsste man aber diese Bitcoins auch an den Staat überweisen können. Wenn aber die Steuerzahlungen grundsätzlich nur in Euro erfolgen können, dann haben Sie schon mal ein Problem - wie wird der Bitcoin dann bewertet, den sie als Unternehmen eingenommen haben. Also das ist eine Geschichte, die gar nicht so einfach zu lösen ist. Also wir müssen dann praktisch einen aktuellen Wert haben, ähnlich wie, wenn Sie als Unternehmen Einnahmen aus Verkäufen haben können wie in Dollar. Dann müsste also dann dieser Dollargewinn des Unternehmens oder diese Dollareinnahme müsste gewertet werden in der Höhe des Wechselkurses zur Eurowährung zu dem Zeitpunkt, wo die Transaktion tätig wurde. Also das ist beim Bitcoin gar nicht so einfach. Da wird diese Problematik, insbesondere wenn Sie einen internationalen Handel betreiben oder Internethandel betreiben noch einmal ungleich schwieriger, aber der Staat hat wie gesagt, ein großes Interesse daran an, diesem Bitcoinsystem zu verdienen, sprich Steuereinnahmen zu erzielen, nur wie er das machen will, das ist mir klar, aber wie das machen will, da scheint es mir noch einige Falschtricks zu geben. Müssen wir abwarten, was er macht, also inwieweit der Staat die Nutzung von Bitcoins regulieren

kann. Das erscheint mir genauso schwierig zu sein wie die generell erstmal zu erfassen, dass die Bitcoins erstmal genutzt werden. #00:31:55-3#

I: Okay. Ja dann bedanke ich mich erstmals. Es waren eigentlich alle meine Leitfragen. Gibt es noch etwas, was Sie zu irgendwas hinzufügen wollten? #00:32:05-4#

Ramb: Ja vielleicht eine grundsätzliche Bemerkung, also vielleicht einmal die ich eingangs gemacht habe. Die Tatsache, dass es Bitcoins gibt und dass die so erfolgreich sind, die basieren halt auf dem tiefen Misstrauen der Menschen in staatliche Währungen und der Staat hat jetzt in seiner, ich sag jetzt mal etwas zynisch, in seiner Arroganz als Hüter der Währungshoheit versäumt, den Nutzern seine Versprechungen an der stabilen Währung oder die Einhaltung seines Versprechens den Nutzern klarzumachen. Das ist ein Fehler, der sich jetzt mehr und mehr zeigt und der sehr verstärkt eben zu diesen alternativen Währungen führt. Wenn Sie so wollen, der Staat ist selbst dran schuld, dass es Bitcoins gibt. #00:32:59-4#

I: Alles klar. Dann vielen Dank für Ihre Zeit. #00:33:03-4#

Ramb: Gerne und ich wünsche Ihnen viel Erfolg. #00:33:03-7#

I: Vielen Dank. #00:33:04#

Anhang 9: Experteninterview Benjamin Kirschbaum

Name	Benjamin Kirschbaum
Institution	Winheller Rechtsanwaltsgesellschaft mbH
Funktionsbezeichnung/Titel	Rechtsanwalt im Bereich Steuer- und Finanzrecht
Kontaktdaten	Unter den Linden 16
	10117 Berlin
	+49 6976757780
	b.kirschbaum@winheller.com
Datum des Interviews	27.11.2017
Freigabe	nicht erforderlich

Interviewer: Ich würde Sie zunächst einmal bitten sich ganz kurz vorzustellen, in meiner Minute beispielsweise Ihren Werdegang und Ihre Berührungspunkte mit dem Thema aufzuzeigen, damit ich Sie in der Bachelorarbeit gut einordnen kann. #00:00:08-9#

Kirschbaum: Ja, also ich bin Benjamin Kirschbaum, jetzt Rechtsanwalt, habe Jura studiert an der „Freien Universität Berlin“, das Staatsexamen mit Prädikat gemacht, dann Referendariat gemacht am „Kammergericht Berlin“, bis zur Rechtsanwaltszulassung, und dazwischen habe ich bei Jakuna gearbeitet, einer jetzt nicht mehr existierenden Bitcoin Börse, und mich davor schon privat mit Bitcoin auseinandergesetzt und gekauft und gehandelt und gemacht Es gab kurze berufliche Berührungen, und ich mache jetzt quasi in meiner Anwaltschaft... Spezialisierung auf Kryptowährungen und alles, was steuerrechtlich und aufsichtsrechtlich da dranhängt. #00:00:47-5#

I: Alles klar, vielen Dank. Dann würde ich sagen, starten wir einmal mit der ersten thematischen Frage. Und zwar würde ich Sie einmal bitten, ganz kurz noch einmal die zentralen Eigenschaften aufzuzählen, die die Blockchain, oder die Blockchain von Bitcoin ausmachen, damit wir da auf einem Stand sind. #00:01:03-9#

Kirschbaum: Also die zentralen Eigenschaften sind meiner Meinung nach, dass es (Anmerkung des Autors: Bitcoin) dezentral ist und dass es mathematisch ist... also das sind die wichtigsten Eigenschaften... mathematisch, kryptographisch... ja also, dass es

keinen zentralen Akteur gibt, der vorschreiben kann, was passiert, und dass die Regeln nicht einfach... subjektiv geändert werden können, sondern klar definiert sind... in einem Open Source, an den sich jeder halten muss. #00:01:27-7#

I: Ok, alles klar. Ich bin dann auch in meiner Recherche, in der ich auch Währungen und Geld definieren muss, darauf gestoßen, was quasi die drei Eigenschaften darstellt. Eine Währung sollte Tausch- und Zahlungsmittel sein, und eine Recheneinheit und Wertspeicherung darstellen. Da ist meine Frage nun, ob Sie das bei Bitcoin überhaupt als gegeben ansehen könnten, oder ob man Bitcoin vielleicht sogar eher als Asset sehen sollte? #00:01:51-3#

Kirschbaum: Genau, also die Kriterien, wo haben Sie die her? Von Hayek, oder? #00:01:56-7#

I: Ich habe da mehrere Quellen gefunden, mehrere Bücher, aus denen ich das zusammengesucht hatte und dabei haben quasi alle das Gleiche bestätigt. #00:02:02-5#

Kirschbaum: Genau also Recheneinheit auf jeden Fall... also Bitcoin ist teilbar, und es ist völlig egal, welchen Bitcoin Sie haben, es ist immer ein Bitcoin... und es macht überhaupt keinen Unterschied, wie jetzt zum Beispiel zu Diamanten... wenn Sie zum Beispiel drei Diamanten haben... gut, weiß kein Mensch. Das ist bei Bitcoin auf jeden Fall gegeben. Tausch- und Zahlungsmittel... das finde ich schon schwieriger. Also ich glaube real mit Bitcoin getauscht und gezahlt wird in der Praxis... wenig. Es ist auf jeden Fall möglich, damit zu tauschen und zu zahlen, aber... ob das in der Praxis angewendet wird bezweifle ich... in größerem Umfang und es gibt ja zum Beispiel „Greshams Law“, dass gutes Geld von schlechtem Geld verdrängt wird... und wenn man bedenkt, Bitcoin wäre gutes Geld, dann zahlt man natürlich lieber mit staatlichem Geld, was ja auch akzeptierter ist... und meine Bitcoins eventuell mehr Wertspeicherung hätten... schwierig. Also, wie lange gibt es Bitcoin jetzt? Fünf, sechs Jahre? Wir sehen eine Wertsteigerung von drei Dollar auf jetzt knapp 9000 Dollar, das ist natürlich jetzt keine Wertspeicherung mehr, das ist schon eine Wertvervielfältigung, aber ich denke, um das als Wertspeicher anzusehen, bräuchten wir eine längere historische, empirische Datenlage. Also wenn wir Gold nehmen, das ist relativ wertstabil über die Jahrtausende, Bitcoin mit fünf Jahren, müssen wir mal gucken, bis zum ersten Absturz, was sich danach ergibt. Und deshalb Währung... zurzeit eher Spekulationsobjekt. #00:03:35-5#

I: Ok, ich greife schon mal eine Frage vor, wenn wir schon bei dem Thema sind. Bitcoin bekommt immer mehr Relevanz und immer mehr Unternehmen bieten Bitcoins als Zahlungsmittel an. Glauben Sie, dass die Akzeptanz dort die nächsten Jahre noch ansteigt? Soweit, dass es als Zahlungsmittel weite Verbreitung findet? Oder glauben Sie andere Kryptowährungen könnten diesen Zahlungsaspekt übernehmen und Bitcoin wird eher als Spekulationsobjekt oder Wertspeicher genutzt? #00:04:01-2#

Kirschbaum: Das ist so ein bisschen Kaffeesatzleserei. Die meisten Unternehmen, die jetzt Bitcoin als Zahlungsmittel angenommen haben, von den größeren Unternehmen, haben das, glaube ich , eher aus Marketinggründen gemacht, als daraus, dass sie wirklich einen Vorteil darin gesehen haben, Bitcoin als Zahlungsmittel einzuführen. Dass es in Zukunft steigt, kann ich mir vorstellen für die internationalen Transaktionen... also wenn ich jetzt ein Unternehmen in den Vereinigten Staaten bin und digitale Güter anbiete für Menschen aus Asien und Europa, dass Bitcoin weniger Wechselkursrisiken hat als zum Beispiel, wenn ich über PayPal zahle oder andere Onlinezahlungsmethoden nutze. Insofern kann ich mir das vorstellen, ob es im innerstaatlichen Zahlungsverkehr Akzeptanz erreicht, im Mainstream, und vor allem innerhalb des SEPA Raums, die jetzt ja auch an 15 Sekunden-Transaktionen arbeiten, wage ich bezweifeln. #00:04:47-2#

I: Also, es wird ja momentan daran gearbeitet, dass bei Bitcoin das Lightning-Network eingeführt wird. Das Ganze wird dann eine Off-Chain Lösung darstellen, die Transaktionen unabhängig von der Haupt-Chain abwickeln und diese dann anschließend erst dem Hauptverzeichnis zuführt. Sollte dies funktionieren, würde es VISA-artige Transaktionen geben und die Gebühren maßgeblich senken. Wenn dies eingeführt wird, sehen Sie dann größere Chancen? #00:05:11-8#

Kirschbaum: Da ist die Frage, ob die Leute das akzeptieren. Wenn sie das nicht begreifen... also wenn ich jetzt mit der VISA-Karte bezahle, dann weiß ich, das Geld geht weg und landet irgendwo bei einem Anderen. Beim Lightning-Network, gut da geht mein Geld weg und landet irgendwo beim Anderen und wird auf dem Bitcoin Layer gesettlet. Dabei muss ich dann ja sowohl bei dem Empfänger diesen Lightning-Network Payment Channel einrichten, als auch bei mir als Sender, und das für jeden einzelnen laden. Wenn das eine unglaublich hohe Usability hat und auf dem Smartphone läuft, dann kann ich mir vorstellen, dass das durchaus Verbreitung finden könnte... wenn es denn überhaupt die Lösung ist. Wir haben ja noch eine andere

Frage... die Konkurrenz zur On-Chain Scalebiltiy zum Beispiel... ja, also unter den Voraussetzungen, dass es eine wirklich hohe Usability hat, und wenig Gebühren hat, für den einzelnen Händler und Nutzer, dann ja. #00:06:08-4#

I: Alles klar, dann würde ich gerne noch einmal auf weitere Eigenschaften schwenken, nämlich welchen Einfluss die noch sehr hohe Volatilität auf Nutzbarkeit von Bitcoin als Handelswährung hat und ob es sich überhaupt lohnt... anstatt zu sparen, dies auszugeben.

Kirschbaum: Angenommen, Sie haben sich jetzt Bitcoin gekauft und es war vor zwei Wochen 7000 Dollar wert und ist heute 9000 Dollar wert... möchten Sie es ausgeben... um sich davon beispielsweise eine Pizza zu kaufen? Eher nicht. Zumal ja dann auch noch die Steuerrechtsthematik dazu kommt. Sobald Sie anfangen Ihre Bitcoins auszugeben, müssen Sie eventuell einen Wertgewinn versteuern, was Sie sonst nicht machen müssen, wenn Sie sich die selbe Pizza mit Euros kaufen. Also alleine die potenzielle Versteuerung Ihres Wertgewinnes, könnte der Nutzung von Bitcoin als Handelswährung derzeit entgegenstehen... und weil das ja ein buchhalterischer Alptraum ist, die Besteuerung der Bitcoins nachzuvollziehen und dies korrekt in die Steuererklärung einzuführen. Allein die Bürokratie da daran hängt, spricht gegen den Nutzen als Handelswährung. Gerade durch die hohe Volatiliät, da ich ja nicht sagen kann, mein Bitcoin war am Anfang des Jahres 100 Euro wert und ist am Ende des Jahres 100 Euro wert, sondern es schwankt jede Woche. Ich muss dabei also anfangen nachzurechnen... wann habe ich diesen Bitcoin gekauft, wann habe ich ihn getauscht und wie viel Steuer muss ich jetzt darauf zahlen? #00:07:39-6#

I: Sehen Sie dabei die hohe Volatilität ausgelöst durch Bitcoin als neues, aufkommendes System an, da Bitcoin jetzt noch eine geringe Marktkapitalisierung hat und sich erst langsam etabliert, oder bleibt die Volatilität aufrechterhalten? #00:08:02-6#

Kirschbaum: Also die Volatilität wird sich wahrscheinlich, sollte es sich als Asset-Klasse etablieren, sinken. Die Frage stellt sich... haben wir zurzeit eine große Volatilität, oder geht es einfach nur volatil aufwärts? Volatilität wäre ja ein Schwanken nach oben und unten, zurzeit schwankt es ja nur nach oben. Aber generell würde ich sagen, dass eine Volatilität im Laufe der Zeit abnehmen muss. #00:08:37-2#

I: Dann würde ich auf die nächste Frage schwenken. Bitcoin ist ja dezentral, das heißt, es gibt keine zentrale Entität, die Preisniveaustabilität oder Wertstabilität

gewährleistet. Das ganze System beruht ja auf dem Vertrauen der Nutzer um sich aufrecht zu erhalten. Sehen Sie dieses unregulierte System als Chance oder als Risiko an? #00:08:59-7#

Kirschbaum: Also ich sehe das eher als Chance an, als als Risiko. Gerade weil sich der Preis von Bitcoin am Markt bestimmen muss, ist die Preisfindung ja den kapitalistischen Kräften ausgesetzt und deshalb wissen wir ja auch... also wir haben kein Versprechen des Staates. Das würde ich gerne ansprechen. Was ist denn das Versprechen des Staates, wenn wir zum Beispiel einen Euro haben? Der Staat garantiert mir zwar... vorgeblich, dass ich morgen für meinen Euro auch etwas bekomme... aber wie viel das ist, dass kann mir der Staat ja auch nicht versprechen. Wir haben ja die Europäische Zentralbank, die ja quasi als Amt für Preisstabilität zuständig ist. Ob die das schafft, weiß kein Mensch. Angesichts auch der hohen Geldmengen, die generiert werden und die ja jetzt auch in den Aktienmarkt und in den Immobilienmarkt fließen, sowie in Kryptowährungen... von daher... bevor ich jetzt eine omnipotente Institution, wie eine Zentralbank brauche, die meine Preisstabilität meiner Währung garantieren will, finde ich schon, dass der Markt mit mehr Playern, die daran mitwirken, mehr Chancen als Risiken bietet. #00:10:36-1#

I: Ok, dann würde ich weiter auf die rechtliche Seite schwenken. Und zwar wäre dort meine erste Frage... bei Bitcoin können Zahlungen nicht rückgängig gemacht werden. Gibt es dabei verbraucherschutzrechtliche Probleme? #00:10:55-5#

Kirschbaum: Also meiner Meinung nach nicht. Wenn Sie etwas kaufen... bei Amazon und das ist jetzt defekt. Dann können auch nicht einfach zur Bank gehen und Ihre Banküberweisung rückgängig machen... also Sie können das zwar technisch, aber Sie dürfen das ja rechtlich gesehen auch nicht. Sie dürfen ja nicht Ihre eigene Zahlung in die Hand nehmen, Sie müssen ja schon die Summe vom Verkäufer zurückverlangen und das im Zweifel vor Gericht einklagen. Sich eigenmächtig seines Geldes wieder zu bemächtigen, funktioniert ja auch so nicht. Da sehe ich überhaupt keine Probleme. Wenn ich als Verkäufer Bitcoin als Zahlungsmittel annehme, defekte Ware liefere, dann kann ich ja von dem Verbraucher, unter denselben verbraucherschutzrechtlichen Regelungen wie beim Kauf mit Euro, verklagt werden und bin dann eben verpflichtet den Verkaufspreis zurückzuzahlen... in Bitcoin dann. Das ist vielleicht sogar eher eine Chance. Die Frage ist, wie viele Bitcoins muss ich zurückzahlen. Wenn ich jetzt eine Ware für drei Bitcoin kaufe, die damals 300 Euro wert war, und jetzt fechte ich an und

erhalte drei Bitcoin für 600 Euro zurück, oder eben weniger als vorher. Das finde ich eher interessant. #00:12:08-4#

I: Das stimmt. Und wie werden dann Käufe generell versteuert? Gibt es da Unterschiede auf der steuerrechtlichen Seite, wenn ich mit Bitcoins bezahle? #00:12:19-1#

Kirschbaum: Also generell nicht. Sie kaufen sich etwas, und ob der Käufer die Zahlung in Bitcoin annimmt, oder in Euro, ist insofern egal. Sie haben natürlich, was wir vorhin angesprochen haben, das Problem, wenn die Bitcoin, die Sie nutzen, um die Ware zu kaufen, zwischenzeitig im Wert gestiegen oder gefallen sind. Dann haben Sie eventuell einen steuerwirksamen Vorgang... soll heißen, Sie müssen auf einmal anfangen, nicht nur die Ware, die Sie jetzt bekommen haben zu bezahlen, sondern auch noch eventuell Steuern für die Wertsteigerung an das Finanzamt. Der Händler hat das Problem, dass er, wenn er Bitcoin als Zahlung annimmt, die Umsatzsteuer an das Finanzamt nicht in Bitcoin zahlen kann. Das heißt er muss irgendwie Euro einnehmen und dann wiederum die Bitcoins eintauschen, was wiederum ein steuerpflichtiger Vorgang sein kann, wenn Wertsteigerung oder Wertsenkung realisiert worden sind. #00:13:08-3#

I: Sehen Sie dabei noch irgendwelche Vor- und Nachteile bei der Nutzung von Bitcoin? Abgesehen von den eben besprochenen Punkten. #00:12:24-8#

Kirschbaum: Also ich glaube, die Vorteile für den Händler sind auf jeden Fall... wenn die Bitcoins erst einmal da sind und bestätigt sind, sind die Bitcoins auch da und es ist bestätigt. Dabei kann es dann nicht, wie wir vorhin gesagt haben, durch Anruf bei meiner Kreditkartenfirma oder bei meiner Bank rückgängig gemacht werden... mit bösartigem Willen. Insofern ist das auf jeden Fall ein Vorteil für das Unternehmen.

Aus Verbrauchersicht gibt es vielleicht auch den Vorteil, dass ich leichter nachweisen kann, dass ich gezahlt habe. Wenn ich einfach auf die Blockchain verweisen kann und sagen kann: „Schaut her, ich habe gezahlt.“, dann könnte das somit auch ein Vorteil für den Käufer sein. #00:14:00-8#

I: Und gibt es dort Unterschiede in meiner Steuererklärung oder muss ich auf andere Dinge achte, wenn ich mit Bitcoins zahle? #00:14:14-1#

Kirschbaum: Im Rahmen der Steuererklärung... also außer das, was wir schon angesprochen haben, dass Sie Wertzuwächse versteuern müssen, die Sie erzielt haben und die Sie dann realisiert haben, indem Sie sich etwas davon gekauft haben, eigentlich nicht. Dem Finanzamt ist es völlig egal ob Sie Ihr Leben über Euro, Bitcoin oder Tomaten bestreiten. #00:14:34-8#

I: Ok, vielen Dank. Dann würde ich von der Steuerseite weg auf die technische Seite gehen. Aktuell gibt es ja sehr lange Transaktionszeiten und auch hohe Gebühren, die kleine Beträge nicht mehr wirtschaftlich machen... also, das würde ich jetzt einmal behaupten, mit Bitcoins zu bezahlen. Die Miner nehmen die Transaktionen mit den höchsten Gebühren. Je niedriger die Gebühren, wenn man es im Wallet einstellen kann, desto länger dauert die Transaktion. Sehen Sie neben dem Lightning-Network dort noch andere Möglichkeiten, dies zu lösen? #00:15:8-1#

Kirschbaum: Die Bitcoin Community hat sich ja über diese Fragestellung gespalten. Es gibt ja Bitcoin Core, die die Lightning-Networks bevorzugen und es hat sich ja Bitcoin Cash abgespalten, die die On-Chain Skalierung befürworten und die Blockgröße von 1MB auf 8MB erhöht haben und jetzt die Probleme, die Bitcoin plagen, gar nicht haben. Mit den jetzt schon zweistelligen Transaktionsgebühren... also, das ist ja lächerlich. Früher hatte man ja gesagt, man kann Bitcoin für internationale Transaktionen verwenden. Das war billiger, als wenn ich eine normale Banküberweisung anschieben würde und inzwischen ist das ja gar nicht mehr der Fall. Also die Sache ist die... ich kann Ihnen nicht sagen, was sich durchsetzen wird, das Lightning-Network oder die On-Chain Skalierung. Ich finde, das ist eigentlich das ganz Schöne an Bitcoin, dass es dezentral und ohne zentrale Entität ist. Also der Markt entscheidet ja tatsächlich, was setzt sich durch, und was ist am besten. Es muss jetzt kein allmächtiger Gesetzgeber kommen, der entscheiden kann und im Zweifelsfall die falsche Entscheidung trifft. #00:16:25-1#

I: Vielen Dank. Damit würden wir auch gleich zur nächsten Frage kommen, nämlich, dass sich die Miner und die Entwickler oft uneinig sind. Als wie fragil sehen Sie das System daher an, wenn es oft zu Auseinandersetzungen auf der politischen Ebene kommt und sich die Entwicklerteams abspalten. Daher die Frage, als wie fragil Sie das System ansehen und wie weit solche Uneinigkeiten führen können. #00:17:01-5#

Kirschbaum: Ja, also das kann natürlich... also bis jetzt hat sich der Bitcoin sehr robust gezeigt. Wir hatten drei Hardforks und Bitcoin gibt es immer noch. Wir hatten bei den Altcoins, zum Beispiel bei Ethereum Hacks, bei denen dort mehrere Millionen Dollar verschwunden oder einkassiert worden sind oder unnutzbar geworden sind und die Währung scheint bisher stärker als nie zuvor. Insgesamt scheint das System sehr robust zu sein und ich glaube... gerade, weil es die Möglichkeit der Hardforks gibt und man, wenn man sich partout nicht einigen kann, sich mehr oder minder friedlich abspalten kann, stabilisiert das System, anstatt es fragiler zu machen. #00:17:46-1#

I: Sehen Sie dabei eine Verwirrung für die Nutzer und für die Menschen, die dort Investitionen tätigen möchten, wenn für jemanden, der nicht komplett im Thema drin ist, nicht ersichtlich ist, welches das Core Team ist und was die verschiedenen Versionen mit sich bringen? #00:18:03-4#

Kirschbaum: Ja, also wenn ich jetzt von außen neu bin, und ich muss mich jetzt entscheiden... kaufe ich Bitcoin, Bitcoin Cash, oder Bitcoin Gold, dann glaube ich schon, dass ich sehr verwirrt bin am Ende. Das ist natürlich schon ein markenrechtlicher Alptraum, dass sich alles Bitcoin nennen kann. Also, dass man sich Bitcoin Cash oder Bitcoin Gold genannt hat, ist ja schon ein Zugeständnis. Man hätte ja auch sagen können, wir sind jetzt der richtige Bitcoin und nennen uns nur Bitcoin. Das kann durchaus für Verwirrung sorgen. #00:18:36-3#

I: Ok, dann erst einmal vielen Dank. Ich habe noch zwei Fragen. Wir waren jetzt auch schneller, als ich gedacht hatte. #00:18:46-1#

Kirschbaum: Soll ich mehr erzählen (lacht)? #00:18:46-2#

I: Wenn Sie noch mehr zu etwas zu sagen haben, dann sehr gerne (lacht). Ich wollte noch einmal fragen, als wie sicher Sie quasi die Nutzung von Bitcoins ansehen. Die Blockchain an sich ist ja sehr sicher, aber die Schnittstellen, wie zum Beispiel die Wallets, wie schon angesprochen, sind da eben noch anfälliger, wenn diese nicht richtig umgesetzt wurden. Bei Ethereum, also bei Parity wurden dann ja... wie viel war das? 150 Millionen, die eingefroren wurden? Als wie sicher sehen Sie da die Nutzung von Bitcoin... abgesehen von der Blockchain? #00:19:21-5#

Kirschbaum: Also die Nutzung von Bitcoin an sich... für jemanden, der weiß, was er tut... und auf gut gewartete Wallets setzt, sehe ich das als... relativ... risikoarm an. Also

seine normale Online-Bank zu benutzen, ist ja natürlich noch risikoärmer... das sind ja alte System, erprobte Systeme, überwachte Systeme... jetzt, wenn man nicht die fancieste und neuste Technologie bei Ethereum ausprobieren möchte, sondern einfach nur seine Bitcoin irgendwo aufbewahren und durch die Gegend schieben möchte, halte ich das Risiko für den normalen Nutzer derzeit für überschaubar. Natürlich wenn man sich auf vernünftige Währungen verlässt, und jetzt nicht die neuesten ICOs mitmachen möchte und sich an die größeren Währungen hält. Gerade Bitcoin als gut gewarteter Code... das funktioniert schon... denke ich. #00:20:19-4#

I: Ich habe zu dem Thema noch eine Frage, und zwar wenn ich jetzt an die breite Öffentlichkeit denke, wie zugänglich sehen Sie Bitcoin da? Es gibt ja schon Startups, bei denen sich die Kunden mit einer VISA-Karte mit Bitcoin vernetzen und damit dann Transaktionen schon umsetzen können und... aber dennoch sollte ja jeder wissen, wie schütze ich meinen Private- und meinen Public-Key und braucht, glaube ich, wenigstens ein kleines technisches Verständnis, um damit sicher umzugehen. Wie gemacht sehen Sie Bitcoin da für die breite Masse? #00:20:55-2#

Kirschbaum: Naja, es ist ja entstanden durch irgendwelche Krypto-Geeks, die sich irgendwelche Krypto-Whitepapers hin- und hergeschoben haben und dann angefangen haben, das Ding zu programmieren. Da steht dann die Usability für den Endkunden in der Programmierung ziemlich weit hinten. Inzwischen ist natürlich eine relativ große Infrastruktur entstanden, zum Beispiel mit, auch in Deutschland regulierten Börsen, wo man sich relativ einfach Bitcoins oder Altcoins gegen Euro kaufen kann, was nicht schwerer funktioniert, als ein normaler Aktienkauf bei einem normalen Aktienbroker... und die Wallets die es für Android oder iPhone gibt, sind inzwischen zu einem größeren Teil auch relativ einfach zu bedienen. Ich denke, dass jemand mit einem gewissen technischen Verständnis... und der etwas Zeit investieren will – ich sag mal – in einem Zeitraum von vier bis sechs Stunden... dass das schon ausreicht um sich ziemlich sicher, als normaler Verbraucher, im Bitcoin Bereich zu bewegen. #00:22:03-3#

I: Ok, dann wäre mir noch ganz kurz eine Frage zur technischen Seite eingefallen, und zwar ob Sie ein Problem in dem immer zentralisierteren Proof-of-Work System sehen. Wird es demnächst sogar vielleicht irgendwann notwendig, dass Proof-of-Stake eingesetzt wird, da Proof-of-Work ja immer mehr an High-End Computer geknüpft wird? #00:22:36-1#

Kirschbaum: Ja... wobei bei Proof-of-Stake haben wir ja die Zentralisierung weg von Proof-of-Stake mit wer hat den größten Rechner, hin zu wer hat den größten Stack. Das ist dann der Matthäus Effekt: Wer hat, dem wird gegeben. Von daher bin ich mir nicht sicher, was besser ist und ob die Zentralisierung der Miner ein Problem ist, oder ob es nicht sogar im Interesse der Miner ist, dass kein einziger Mining-Pool über 51% Rechenleistung sowieso kommt. Also, dass man sich aus Eigenschutz, damit man die Währung sicher hält, limitiert... in der Anzahl an Rechenkraft, die man selber auf sich akkumuliert. #00:23:20-3#

I: Wobei sich dann ja auch Absprachen ergeben können #00:23:25-9#

Kirschbaum: Ja natürlich. Das ist natürlich das nächste Problem, bei dem ja auch gesagt worden ist, dass zum Beispiel die Abspaltung von Bitcoin Cash oder Bitcoin Gold, also Leute, die eigenmächtig das Protokoll ändern wollen... gegen die Developer quasi eine 51% Angriff darstellen... wenn es denn genügend Miner sind. Also, das ist natürlich ein Problem und das ergibt sich ja natürlich auch bei Proof-of-Stake. Ich weiß nicht wie... bei den Minern gibt es ja zumindest... ich weiß, wie viel Rechenkraft gibt es und wie ist die verteilt. Bei Proof-of-Stake weiß ich nicht, wie viele Gruppen oder Personen einen Stake halten und wie viel sie tatsächlich haben. Also nur, wenn ich jetzt auf der Blockchain sehe, es gibt 10 große Wallets, die jetzt 51% meinetwegen auf sich vereinen, dann weiß ich trotzdem nicht, wem die letztendlich gehören. Ist das nur eine Person? Sind das drei Personen? Kennen die sich? Arbeiten die zusammen? Von daher finde ich Proof-of-Work als relativ transparentes Protokoll ganz angenehm. #00:24:28-2#

I: Ja, wobei man ja bei Proof-of-Stake sagt, dass dadurch nicht die Rechenleistung gekauft werden muss, sondern wenn man in Proof-of-Stake mit einem großen Geldbeutel mehr Kosten hat um zu manipulieren... dass das weitaus teurer wäre, da man sich 51% der Währung kaufen müsste, was bei einer großen Kryptowährung wie Bitcoin weitaus teurer wäre. Würden Sie daher also sagen, Transparenz ist dabei wichtiger als mögliche unbekannte Angriffe mit weitaus höheren Budgetanforderungen? #00:25:01-4#

Kirschbaum: Ja... also das müsste man mal ausrechnen, was teurer und was billiger ist. Ich glaube, wenn ich über Proof-of-Work angreifen möchte... ist glaube ich der Zeitaufwand höher, als mir schnell 51% der Währung zusammenzukaufen. Also, auch wenn es wahrscheinlich weitaus teurer ist... angenommen die Leute sind gewillt, mir so viele Bitcoins zu verkaufen, die bekomme ich auf der Börse mit wenigen Mausklicks

zusammen während ich, wenn ich mit Proof-of-Work einen Angriff starten will, erst einmal bei NVIDIA oder AMD anrufen muss, ob die mir überhaupt genügend Grafikkarten zur Verfügung stellen. Also... ich sehe, dass beides Vor-und Nachteile hat... zum Glück muss ich es nicht entscheiden und wir werden dann irgendwann sehen, was sich dann durchsetzt. #00:25:52-3#

I: Vielen Dank. Meine letzte Frage wäre noch... die hat sich jetzt im Interview ergeben und steht auch nicht im Leitfragen drin, als wie reguliert Sie Bitcoin sehen. In Japan gibt es ja viele Gesetze, die Börsen betreffen. Das ist in Deutschland ja noch nicht so geregelt, da hängt Deutschland nach meiner Recherche noch hinterher. Sehen Sie dabei noch Regelungen, die folgen werden? #00:26:31-1#

Kirschbaum: Ich glaube, der Eindruck, dass Börsen von Bitcoin, oder Kryptowährungen in Deutschland nicht reguliert sind... täuscht, also glaube ich zumindest. Da die BaFin Bitcoin und andere Kryptowährungseinheiten ja als Recheneinheiten und damit als Finanzinstrumente im Sinne des Kreditwesengesetzes eingestuft hat, ist ja quasi jeder, der in größeren Mengen mit Kryptowährungen handelt, oder einen Marktplatz anbietet... läuft ja immer Gefahr von der BaFin als Finanzdienstleistungsunternehmen eingestuft zu werden und deswegen eine BaFin-Erlaubnis zu brauchen. Deswegen gibt es ja so wenig... deswegen ist Deutschland ja auch eine Leerstelle, was Bitcoin-Geldautomaten anbelangt. Sobald Sie ins europäische Ausland fahren, sehen Sie überall Bitcoin-Geldautomaten – in Deutschland sehen Sie keinen einzigen, weil natürlich niemand eine BaFin-Erlaubnis dafür bekommt. Von daher denke ich nicht, dass die Regulierung hinterher hängt, was den Umfang der Regulierungen anbelangt, sondern ich denke eher - umgekehrt wird ein Schuh draus – man müsste gucken, ob man Kryptowährungen nicht aus der Banken- und Finanzdienstleistern rausnimmt und und ein eigenes Regelwerk schafft, das vielleicht ein bisschen Start-Up freundlicher ist, als das starre Bankensystem, das ja eigentlich für ganz andere Anwendungsfälle konstruiert worden ist. #00:27:42-1#

I: Wissen Sie spontan, ob Bitcoin von der Deutschen Regierung als Währung eingestuft wird oder eher als Asset... oder wie das da gehandhabt wird? #00:27:48-2#

Kirschbaum: Soweit ich weiß wird es von der Regierung tatsächlich erst einmal als gar nichts eingestuft... und dann kommt es tatsächlich darauf an, wo wir uns befinden. Also befinden wir uns im Steuerrecht, im Einkommenssteuerrecht, dann ist es ein normales

Wirtschaftsgut, wie ein Oldtimer oder ein Kunstgegenstand. Sind wir im Umsatzsteuerrecht, dann hat der EuGH ja befunden, dass es als Zahlungsmittel einzustufen ist, und deshalb von der Umsatzsteuer zu befreien ist. Befinden wir uns im Aufsichtsrecht, dann sind wir eben beim Finanzinstrument... und eventuell, wenn ich jetzt anfange irgendwelche Equity-Tokens auszugeben, dann sind wir vielleicht irgendwann sogar im Wertpapierrecht, oder im Vermögensanlagengesetz. Also, es kommt immer darauf an, in welchem Rechtsgebiet wir uns jetzt befinden. Eine offensichtliche Verlautbarung der Bundesregierung zu – wie ist Bitcoin in jedem Fall einzustufen – ist mir nicht bekannt... und existiert denke ich auch nicht. #00:28:41-1#

I: Ja, vielen Dank für das Interview. Das wären jetzt erst einmal meine Fragen. #00:28:47-4#

Anhang 10: Experteninterview Patrick Charrier

Name	Patrick Charrier
Aktuelle Institution	Blockchain Helix
Funktionsbezeichnung/Titel	Blockchainentwickler - Backend
Kontaktdaten	K.A.
Datum des Interviews	28.11.2017
Freigabe	nicht erforderlich

I: Guten Tag Herr Charrier. Vielen Dank, dass Sie sich die Zeit nehmen. #00:00:03-7#

Charrier: Also, für mich ist es ok, wenn wir uns duzen, da habe ich kein Problem mit... das macht die Sache, glaube ich einfacher. #00:00:5-9#

I: Alles klar. Ich möchte Dich am Anfang einmal bitten, damit ich Dich in der Bachelorarbeit gut einordnen kann, eine halbe Minute ganz kurz deinen Werdegang zu beschreiben und deine Berührungspunkte mit dem Thema. #00:00:09-4#

Charrier: Ok, also beruflich komme ich, oder von dem was ich studiert habe, komme ich aus einem ganz anderen Umfeld. Meine Grundinteressen lagen eigentlich immer in der Computergrafik/Computersimulation... und das habe ich auch studiert. Das Fach, das ich studiert habe, heißt „Computational Engineering“. Ja, aber es war so, dass ich 2012 zum ersten Mal von Bitcoin gelesen habe... und weil ich das Konzept halt irgendwie cool fand, habe ich auch gleich ein paar gekauft und war dann relativ überrascht, als dann 2013 die erste „Mega Blase“ kam... aber gleichzeitig habe ich auch gesehen... diese Technologie kann viel mehr als nur Geldsysteme abbilden. Ich habe quasi schon am Anfang relativ schnell erkannt, dass es die Büchse der Pandora ist. Sobald es einmal geöffnet ist, wird sich... kann man damit alles verändern. Dann kam ja diese tiefe Depression 2013/2014, drei Jahre lang ging der Kurs ja immer nur runter und erst im letzten, oder im vorletzten Jahr, ich weiß es gar nicht mehr genau, ging der Kurs dann langsam wieder hoch. Teil meiner Coins hatte ich schon direkt nach der Blase verkauft, einen Teil habe ich aber tatsächlich diese ganzen drei Jahre durchgehalten, was ganz nett war. Ja, dann war ich mit meinem Studium fertig und habe meine Promotion angefangen, die ich allerdings Anfang dieses Jahres abgebrochen habe. Zum einen, weil... also das hatte mit der Promotion selbst zu tun...

die Finanzierung hatte nicht gestimmt usw. Ich war einfach nicht so ganz zufrieden, aber gleichzeitig ist natürlich dann 2016 dieser Hype mit Ethereum losgegangen mit den ganzen Altcoins. Ich war da natürlich mit einem Fuß noch in den Kryptowährungen drin und für mich war das dann auf einmal wie ein Traum... auf einmal ist dieses ganze Ökosystem entstanden... und ich bin dann da auch wieder eingestiegen, sodass ich jetzt im April überlegt habe, ob ich das Ganze nicht auch beruflich machen will, also vollberuflich als Blockchain Entwickler. Mit Ethereum kamen ja dann die Smartcontracts auf und das habe ich mir relativ schnell beigebracht. Kurse an sich gibt es ja nicht so wirklich. Ich glaube, es gibt noch so... Seminare in denen das angeboten wird. Da legt man dann aber schon mal 10.000 Euro hin... also nicht günstig. Aber man kann sich das auch, sofern man Entwicklererfahrungen hat, selber beibringen. Das habe ich gemacht und bin dann zum ersten Meet-Up gegangen, die dann auch langsam aufkamen und habe dann jemanden kennengelernt, der gemeint hat, er kennt da eine Firma in Frankfurt namens „Blockchain Helix“, die wollen ein Identitätsmanagement mit der Blockchain bauen und ob ich da nicht mitmachen wollte. Und ja, seitdem sind quasi Smart Contracts mein A und O jeden Tag. Das ist so der aktuelle berufliche Werdegang. Ach so... ich habe dort eine 50% Stelle, weil ich das Gefühl habe, dass ich auch noch andere Projekte gerne machen würde. Zum einen eine Miningfarm in Tschechien, da bin ich schon mit einem Freund aus Würzburg relativ lange dran und zum anderen hat mich die Firma Crytek, eine Spieleentwickler-Firma, angesprochen, die möchten ein ICO für eine Rewardsystem bauen. Da geht es darum, Reviewer und App-Creator zu matchen und ein möglichst konfliktfreies Reviewsystem zu bauen, auch mit Tokens incentiviert und eleganter abgebildet, als dies aktuell der Fall ist. Genau... ich bin da also gerade mittendrin in diesem ganzen... Wahnsinn. Es ist auch nicht immer alles schön, sondern wie der Wilde Westen, aber an sich... mir liegt es irgendwie... es ist genau mein Ding, obwohl ich aus einer anderen Richtung komme. #00:04:57-9#

I: Ok, dann erst einmal vielen Dank für die Vorstellung. Ich würde sagen wir springen direkt zur ersten... einleitenden und technischen Frage, welche zentralen Eigenschaften Bitcoin und dessen Blockchain nun eigentlich ausmachen. Da würde ich Dich bitten, das einmal ganz knapp zusammenzufassen. #00:05:17-8#

Charrier: Das Besondere ist natürlich – es ist dezentral. Zweitens – es ist transparent, das heißt, alles ist für alle nachvollziehbar. Insofern kann man es auch nicht fälschen und es ist langlebig. So sehe ich Bitcoin – zusammengefasst. #00:05:36-1#

I: Ok. Bei meiner Recherche bin ich auf die Frage gestoßen, dass eine Währung die folgenden drei Kriterien erfüllen müsste: Tauschmittel, Recheneinheit und stabile Wertspeicherung. Da lautet meine Frage jetzt: „Siehst Du das überhaupt als gegeben an?“ Bitcoin und andere Kryptowährungen werden ja immer als *Währungen* bezeichnet werden, oder würdest Du eher sagen, das (Anmerkung des Autos: Bitcoin) ist ein Asset, und warum? #00:06:01-5#

Charrier: Also der Begriff Währung trifft auf Bitcoin nicht mehr zu, auf andere Krypto-*Währungen* schon, aber dadurch, dass die Transaktionskosten so gestiegen sind, ist es als Tausch-und Zahlungsmittel nicht mehr einsetzbar (Anmerkung des Autors: zu dem Zeitpunkt des Interviews [Stand: 29.11.2017] waren die Transaktionskosten kurzzeitig doppelt so hoch [ca. 6$ pro Transaktion] wie der Durchschnitt). Interessanterweise, oder absurderweise findet es jetzt bei großen Anbietern, wie Amazon oder Microsoft auf einmal doch Verwendung als Zahlungsmittel, was ich nicht ganz nachvollziehen kann. Ja, aber ich sehe es nicht mehr als Währung, sondern wenn überhaupt diesen Punkt Wertspeicherung, der im Sinne von Gold... wahrscheinlich in der Kategorie liegt. #00:06:45-1#

I: Ok, dann würde ich gerne Frage neun aus dem Fragenkatalog (Anmerkung des Autors: Der Interviewpartner bat vorab um einen Fragenkatalog) vorgreifen, also als wie lösbar Du die aktuellen Transaktionszeiten siehst. Die Miner nehmen sich die Transaktionen mit den höchsten *Fees* und je höher diese, desto schneller wird die Transaktion bearbeitet und je geringer, desto höher ist dabei die Wartezeit. Würdest du sagen, dass dies mit dem Lightning-Network lösbar ist, oder siehst du dabei noch andere Alternativen? #00:07:03-8#

Charrier: Ja, also es ist technisch definitiv lösbar. Da gibt es, wie gesagt das Lightning-Network, das ist ein Ansatz. Es gibt aber auch noch das *NG-Protokoll* (Anmerkung des Autors: Bei dem NextGenerations-Protokoll handelt es sich um einen Ansatz, bei dem die Blöcke nicht alle 10 Minuten akzeptiert werden, sondern Miner vorausschauend winzige Blöcke mit jeweils einer Transaktion kreieren, die dann von einem, alle 10 Minuten zufällig auserwählten Miner zu einem großen Block zusammengefügt werden können. Dies hat kurzgesagt ähnliche Vorteile wie das Lightning-Network und stellt eine andere Herangehensweise dar) zum Beispiel... es gibt ganz viele Ansätze die Transaktionszeiten zu verringern, oder auch günstiger zu machen, aber es ist eher eine politische Frage, wie wir immer wieder sehen. Das ist auch so eine interessante Eigenschaft, habe ich mal gelesen... am Anfang dachte man, dass mit einer dezentralen Währung auch alle politischen Probleme gelöst sind, aber das stimmt

natürlich überhaupt nicht, die Politik findet natürlich auch da dann wieder statt. #00:07:43-5#

I: Das bezieht sich auch fast genau auf Frage 12, also als wie fragil Du das System ansiehst. Die ganzen Uneinigkeiten, jetzt zum Beispiel auch bei Bitcoin Cash (Anmerkung des Autors: Ein Teil des Bitcoin Core Entwicklerteams hat sich, Zwecks Meinungsverschiedenheiten über die Zukunft und Funktion von Bitcoin, mit einer Hardfork gespalten) und auch die vermeintlichen Hintergrundmotive, warum solche Aktionen durchgeführt werden. Siehst du das System als stabil an? #00:08:05-9#

Charrier: Ok, genauer formuliert meinst du damit, dass die Verteilung des Kapitals immer zentralisierter wird, und auch, dass die Hashing-Power immer zentralisierter wird? #00:08:29-1#

I: Unter anderem. #00:08:30-1#

Charrier: Das ist eine interessante Frage, weil... ich finde, auch da ist wieder die Analogie zum normalen Geldsystem. Um zu erinnern, auch in der normalen Welt haben 1% der Menschen 50% des Guthabens, und kontrollieren wahrscheinlich auch in großer Art und Weise die Politik und damit auch die Regeln – und das ist für mich die exakte Analogie auch zu Bitcoin. Auch hier findet sich wieder eine kleine Elite, die die Kontrolle über das System übernimmt... in gewisser Weise und das ist für mich eigentlich ein sehr natürlicher Prozess und ich glaube, dass mit allen Geldsystemen genau das hier am Ende passiert, was man hier jetzt wieder beobachten kann. Das wäre meine Theorie dazu. #00:09:25-5#

I: Würdest Du das, was da bei Bitcoin Cash passiert ist, als Marktmanipulation ansehen? #00:09:31-3#

Charrier: Also, meine Antwort hat sich nicht auf Bitcoin Cash bezogen, sondern generell... dass das Kapital immer zentralisierter ist und dass die Mining-Power immer zentralisierter ist. Das empfinde ich als einen ganz normalen Prozess im Geldsystem. Bei Bitcoin Cash habe ich mich ehrlich gesagt überhaupt nicht damit beschäftigt. Da ging es darum die Blöcke von 1MB zu erhöhen oder? #00:10:07-1#

I: Genau, von einem Megabyte auf acht Megabyte, aber viele haben denen (Anmerkung des Autors: Entwicklerteam Bitcoin Cashs) vorgeworfen, dass all

das nur ein Vorwand war, eine Hardfork zu generieren, um mehr Geld reinzuholen. Und der Code war wohl auch sehr schlecht geschrieben und enthielt nicht einmal Replay-Protection (Anmerkung des Autors: Vorgang, bei dem Bitcoins und Bitcoin Cash aus Versehen gleichzeitig von einem Wallet versendet werden), was aus meiner Sicht eigentlich ein großes Manko darstellt. Aber sonst würde ich auf eine andere Frage zu sprechen kommen. Wir waren ja gerade bei Proof-of-Work - siehst du in dem immer zentralisierteren Proof-of-Work System ein Problem und würde Proof-of-Stake dabei Abhilfe schaffen? Laut vielen Meinungen sei es ja schwerer und teurer mit Proof-of-Stake 51% zu erreichen, als wenn man Hardware für eine 51%-Attacke mittels Proof-of-Work durchzuführen versucht. Wie siehst du das? #00:10:58-4#

Charrier: Sehe ich auch so. Bei Proof-of-Stake hat man leider die Gewissheit, dass irgendwann eine 51%-Attacke möglich wird, wenn man das ausrechnet, liegt die Zeit allerdings bei ungefähr 2000 Jahren, habe ich in einem Artikel gelesen. Es ist absolut unwahrscheinlich, dass jemand mit Proof-of-Stake das System übernimmt. Aber natürlich gefällt mir der Aspekt *Energie* deutlich besser bei Proof-of-Stake, weil Proof-of-Work schon jede Menge Energie frisst, die eigentlich unnötig ist. Da ist ja nichts Produktives dabei. #00:11:39-3#

I: Ok, ich würde noch einmal zu dem Thema Hardforks zurückschwenken. Siehst Du da mögliche Verwirrungen für Außenstehende, die da nicht wirklich tief in dem Thema drinstecken? Wenn zum Beispiel Bitcoin Cash sich als Bitcoin anpreist, wenn es beispielsweise gegoogelt wird? Schreckt es ab, wenn es zu viele Ausprägungen von einem Coin gibt? #00:12:00-2#

Charrier: Natürlich ist es abschreckend, aber auf der anderen Seite finde ich es auch ehrlich. Man kann hier ganz schön sehen, dass der Markt hier alles am Ende regelt. Also die politische Frage: „Ist ein Hardfork richtig oder falsch?“, ist streng genommen gar nicht nötig. Man muss es nicht auf politischer Ebene regeln, sondern der Markt ist in der Lage, diese Frage sehr elegant zu beantworten. Dieser hat ja jetzt auch eine ganz gute Zwischenlösung gefunden... also ich sehe das gar nicht so eng wie die meisten, so verbissen. Der Markt regelt das Ganze. #00:12:46-8#

I: Ok, dann würde ich gerne noch auf ein weiteres Thema am Markt eingehen. Bitcoin ist ja relativ volatil, obwohl eher volatil nach oben. Würdest Du sagen, es ist wirtschaftlich für ein Unternehmen oder einen Endkunden Bitcoin zu nutzen? #00:12:00-3#

Charrier: Wirtschaftlich – naja, aufgrund der Transaktionsgebühren, die ja jetzt mit dem Preisanstieg auch zusammenhängen - nein als Zahlungssystem, aber die Volatilität an sich ist auch ein Riesenproblem. Also ich würde es (Anmerkung des Autors: Bitcoin) nicht als wirtschaftliche Währung bezeichnen. Klar, wenn es immer hochgeht, wie aktuell, dann kein Problem, aber die Erfahrung zeigt halt, dass auch diese Bärenmarktphasen (Anmerkung des Autors: Abwärtstrendmarktphasen) kommen und die nächste kommt vielleicht bald... ist (Anmerkung des Autors: Bitcoin) für mich vielleicht nicht das wirtschaftliche Zahlungssystem der Zukunft. #00:13:48-5#

I: Gehst Du davon aus, dass wenn die Marktkapitalisierung weiter zunimmt, die ist ja im Moment relativ gering. Würdest du sagen, dass dies etwas verändern wird, dass die Prozesse am Markt aktuell als Geburtswehen gesehen werden können und es sich zunehmend stabilisiert? #00:14:06-5#

Charrier: Es gibt noch eine andere Perspektive, und zwar, wenn man sich den Bitcoinkurs logarithmisch anschaut, dann hat man eine Art Baselinegerade und die ist tatsächlich sehr gerade. Man kann auf dieser Geraden genau sehen, dass dieser Preis eigentlich nie überschritten wurde, der sich auf der Geraden logarithmisch abzeichnet, aber auch, dass das aktuell wieder eine Blase ist. Das bedeutet, der Preis, wenn man von dieser Geraden ausgeht, würde bei circa 2000 Dollar liegen, aber jetzt sind wir bei 10.000 Dollar. Da kann man dann schon eine gewisse Blase sehen. Wenn man von dieser Geraden ausgeht, dann glaube ich, dass man langfristig gesehen das schon als Wertspeicher sehen kann und dass man das auf Dauer nicht verlieren kann (Anmerkung des Autors: Den Wert der Bitcoins). Das ist so meine Einstellung dazu. #00:15:21-1#

I: Ok, dann wäre meine nächste Frage in diesem Fall gesellschaftlich gesehen, als wie massentauglich Du Bitcoin ansehen würdest. Man benötigt ja schon ein kleines technisches Verständnis um zu wissen, wie man seine Bitcoins sichern muss und was ein Public- was ein Private-Key ist. Das sollte dann ja jedem geläufig sein, der damit handelt oder umgeht, um sich nicht Gefahren auszusetzen. Wie adaptierbar für die Masse schätzt Du das ein? 00:15:49-3#

Charrier: Für mich ist das so ein bisschen das Henne Ei Problem. Natürlich sind Leute nicht gewöhnt aktuell mit Public- und Private-Key umzugehen, aber für mich stellt sich die Frage, können sie das nicht langfristig lernen? Ist es vielleicht irgendwann genauso normal wie eine E-Mail zu schreiben? Hardware, wie die Trezor- oder Ledgerhardware

(Anmerkung des Autors: Hardwarewallets), verhindern ja zumindest, dass jemand gehackt wird. Das ist schon einmal ein großer Fortschritt. Auch wenn es ein bisschen *clumsy* ist, also auch, wenn es ein bisschen sperrig ist damit umzugehen, ist zumindest das Hauptproblem, dass die Coins gestohlen werden können, gelöst, jedenfalls von meiner Sicht aus. Aber klar, es ist ein Riesenschritt. Auf der anderen Seite... ich glaube schon, dass Menschen, also auch die Masse, lernfähig ist und man hat ja auch gelernt mit Aktien umzugehen, oder mit Fonds und ich denke auf Dauer werden Kryptowährungen auch Standard werden, bzw. kann man sie auch in bestehende Instrumente, wie ETFs einbinden, was ja auch schon passiert und damit wird denke ich die Massentauglichkeit definitiv erreicht. #00:17:28-3#

I: Ok, dann wäre meine nächste Frage als wie sicher Du das System ansiehst. Die Blockchain wurde ja in sieben Jahren nicht gehackt, aber es gibt ja Software-Wallets, die da relativ anfällig sind. Bei Ethereum war es *Parity*, wo jemand mit dem Code gespielt und Ether im Wert von 150 Millionen Dollar eingefroren hat. Da wäre meine Frage, wie sicher Du die Wallets, oder Schnittstellen zur Blockchain siehst? #00:17:53-5#

Charrier: Ich würde da unterscheiden in die Systeme, die Smart Contracts unterstützen und eben die, diese nicht unterstützen, wie Bitcoin. Smart Contracts sind für mich ein gigantisches Kartenhaus, das sehr idealistisch ist und tatsächlich auch eine schöne neue und utopische Welt baut, aber als Entwickler weiß ich, dass man immer Fehler macht. Ich habe noch keinen so vielversprechenden Ansatz gesehen, der garantiert, dass Smart Contracts bugfrei sind. Auch dieser letzte Hack war ja quasi durch einen Bug, es war ja kein Hack, sondern eher ein Bug ausgelöst. Das sehe ich schon sehr kritisch, allerdings glaube ich, dass durch viele Fehler, viele schmerzhafte Fehler, natürlich ein Lernprozess eintreten wird, wenn man immer wieder dieselben Cotract-Bausteine einsetzt und die über die Zeit geprüft werden, dann kann das schon funktionieren. Da sehe ich eine ganz neue Klasse von Entwicklern aufkommen, die sehr viel Verantwortung tragen in der Zukunft. So einen Smart-Contract zu verwalten ‚könnte sich in der Zukunft so ein bisschen anfühlen... wie Gott zu spielen. Die normalen Währungen, jetzt nicht mit Smart-Contracts... für mich ist die Antwort darauf eben diese Ledger-Technologie, also die spezialisierte Hardware. Die kann natürlich immer noch verloren werden, aber es ist schon mal ein Fortschritt. Man kann aber auch hier wieder das alte Treuhänderprinzip einführen. Im Prinzip ist ja die Bank Treuhänder für mein Geld oder Dein Geld. Das kann man hier natürlich wieder auch machen. Vielleicht wird eine Funktion in der Zukunft sein, Private-Keys zu verwalten.

Man sieht es schon bei einigen Unternehmen, die genau solche Services anbieten. Ich denke dieses Problem wird irgendwie umgangen werden. #00:20:29-1#

I: Dann möchte ich noch einmal weiter auf die Nutzung eingehen, und zwar, dass Zahlungen ja nicht rückgängig gemacht werden können. Siehst du da Vor- und Nachteile für Unternehmen, die sich dabei ergeben können? #00:20:40-8#

Charrier: Ja, in der Tat. Ich habe mit Softwaresystemen gearbeitet, wo es nur um so etwas Triviales wie die Verwaltung von Passwörtern ging und selbst da... man muss immer davon ausgehen, dass alle Fehler, die irgendwie möglich sind, gemacht werden und Kryptowährungen bieten natürlich ganz viel Angriffsfläche für Fehler. Da sehe ich in der Tat einen Riesenangriffspunkt für die Massentauglichkeit... sehe ich sehr problematisch. Das bedeutet auch: Wie bildet man Sachen wie Internethandel und Betrug ab? So etwas, das PayPal ja ganz gut gelöst hat... naja, einigermaßen. Da gibt es zwar einige Konzepte. Man kann einen Treuhändertausch machen... ohne Treuhänder. Es gibt für alle Konzepte die wir aus der normalen Welt kennen, nämlich dieses Treuhänderprinzip, wie bei PayPal. Da gibt es auch ein dezentrales Prinzip. Da ist schon Hoffnung da, aber ich glaube nicht, dass sich das in den nächsten 10 Jahren durchsetzt. #0022:16-2#

I: Noch einmal bezogen auf die Nutzung, wie einfach schätzt Du als Softwareentwickler die Zahlung im Internet, beispielsweise für den E-Commerce, mit Bitcoin als Zahlungsmittel ein? Bei Ethereum gibt es zum Beispiel *MetaMask*, ein Browser-Plugin. Gibt es da ähnliches für Bitcoin und siehst Du hierbei noch Probleme? #00:22:45-4#

Charrier: Also, ich habe so etwas tatsächlich mal genutzt. Das ging eigentlich relativ schnell, ungefähr 10 Minuten, also genau die 10 Minuten, die Bitcoin für seine Blockzeit braucht. Manche Zahlungssysteme nehmen schon einfach die Transaktionen, und sind schon damit zufrieden, da geht es sofort. Bei mir ging das erstaunlicherweise relativ schnell. Da sehe ich bei der Integration in den Online-Handel kein Problem, das fließt. #00:23:39-1#

I: Danke, dann möchte ich schnell zur nächsten Frage gehen. Und zwar bezogen auf die Relevanz. Da ergibt sich ja eine Art Teufelskreis. Damit mehr Käufer Bitcoin nutzen möchten, sollten mehr Verkäufer die Zahlungsmethode anbieten, aber damit mehr Verkäufer die Zahlungsmethode anbieten, sollten mehr Käufer Bitcoins nutzen und diese Zahlungsmethode nutzen wollen. Wie wahrscheinlich

siehst du einen maßgeblichen Anstieg der Akzeptanz an, damit die Nutzung steigt? #00:24:08-7#

Charrier: Ich sehe da wieder das Henne Ei Problem und ich glaube, ich sehe die Anzeichen, dass sich die Akzeptanz immer mehr verbreitet. Es gibt ja immer mehr Krypto-Millionäre... und die wollen ja auch etwas mit ihrem Geld machen und das wissen ja auch natürlich die Unternehmen. Ich sehe vielleicht einen großen Bereich in Luxusgütern, dass vielleicht ein Tesla bald mit Bitcoin gekauft werden kann, oder Gucci. Ich glaube, damit wird es anfangen. Es wird erst einmal eine Art Elite-Status sein, mit Bitcoin bezahlen zu können, aber dann, wie bei allem, wird sich dieser Elite-Status langsam nach unten fortsetzen und eine große Akzeptanz finden. #00:25:13-2#

I: Ok, nun ist Bitcoin ja als Netzwerk auch komplett transparent. Siehst Du da eine Hemmschwelle, dass Unternehmen nicht wollen, dass andere nachvollziehen können, wer was an ihre Adresse überwiesen hat, und wie viel sich darauf befindet? #00:25:32-9#

Charrier: Ja, das ist schon ein großes Problem. Wobei... es kommt darauf an, wie die Unternehmen damit verfahren werden. Wenn sie das Geld sofort auszahlen lassen... na gut, dann wäre es immer noch nachvollziehbar, wie viele Einnahmen sie hatten. Ja, da hast du Recht, das ist in der Tat ein Riesenproblem. Es gibt natürlich Währungen wie *Monero*, bei denen man das nicht sieht. Auf der anderen Seite, große Aktienkonzerne müssen ja sowieso ihre Zahlen offenlegen. Also was spricht dagegen? Die andere Seite ist natürlich die Anonymität der Kunden. Ob jetzt ein russischer Großmogul gerne hätte, dass man weiß, was er gekauft hat, wage ich zu bezweifeln. #00:26:39-4#

I: Alles klar, dann würde ich zu meiner letzten Frage kommen. Wir hatten ja schon angesprochen, dass Bitcoin als Blase gesehen werden kann. Die Währung beruht ja quasi nur auf dem Vertrauen der Nutzer in das System... dass es sich hält. Dabei gibt es keine zentrale Entität, wie die EZB oder die IMF, die Wertstabilität garantiert. Siehst Du das eher als Chance oder eher als Risiko? Oder vielleicht beides? #00:27:02-9#

Charrier: Ok, ich persönlich glaube nicht an Regulierungen in dem Sinne, dass sie funktionieren [lacht]. Ich glaube, dass Regulierungen niemals wirklich regulieren können. Ich glaube, dass der Anspruch, eine Währung regulieren zu können, übertrieben ist... ich glaube, dass Regulierung nur die Risiken verschieben kann. Man

kann auch argumentieren, dass die traditionelle Situation mit Kreditblase und Verschuldung schlimmer ist, als 2007 und die ganzen Zentralbankmaßnahmen nur dazu geführt haben, das Problem zu verschieben. Man spricht auch von sogenannten *Hidden Risks*. Regulierung klettet die kleinen Risiken, also genau die Volatilität, die man in Bitcoin sieht... das wird alles schön weggeklettet... aber auf lange Sicht sind sogar die Fiat-Währungen nicht vor echten Crashs sicher. Ich hatte es auch einmal nachgeschaut vor einer Weile: Die durchschnittliche Lebensdauer einer Fiat-Währung liegt bei 27 Jahren. Das muss man sich einmal überlegen [lacht]. Insofern sehe ich Regulierung kritisch. Ich glaube, dass Währungen immer instabil sind, dass sie immer im Wettbewerb miteinander stehen, dass auch hier der Markt entscheidet, welche Währung überlebt und welche nicht. Insofern sehe ich dort keine Überlegenheit von Zentralbankwährungen gegenüber Bitcoin. Vielleicht kann es sein, dass Bitcoin sich relativ schnell verabschiedet – vielleicht übernimmt eine andere Kryptowährung. Das weiß ich nicht. Ich sehe da keinen besonderen Vorteil. Was man natürlich argumentieren kann... bisher kennen Kryptowährungen sowas wie, sagen wir mal Steuern oder Soziales nicht. Das bedeutet, dass im traditionellen Währungssystem ja relativ viel abgeführt wird, um die Infrastruktur für alle zu erhalten und um Projekte damit zu steuern, die allen zu Gute kommen. Das gibt es bei Fiat-Währungen natürlich nicht (Anmerkung des Autors: Kryptowährungen). Das ist, wenn man so will, der reine Kapitalismus – der reine freie Markt. Aber da sieht man auch mit *Dash*, dass es auch andere Ansätze gibt, dass man eine Art Steuersystem in Kryptowährungen einbaut, damit man damit auch Gesellschaftssysteme aufrechterhalten kann. Bei Dash wird es zum Beispiel eingesetzt, um es weiterzuentwickeln oder Dash zu promoten. Ich sehe da schon eine Art Gesellschaftsform drin. Es ist nicht nur eine Währung, sondern eine Art System. Aber meine grundsätzliche Antwort ist: Ich sehe Regulierung nicht als Vorteil, es ist ein alternativer Ansatz. Grundsätzlich: Der Markt entscheidet auf lange Frist. #00:30:51-1#

I: Geht's Du davon aus, dass der Staat bald spezifische Gesetze erlässt. In Japan ist der Markt ja komplett durchreguliert. Werden Deutschland oder Europa demnächst... Kryptogesetze auffahren? #00:31:04-7#

Charrier: Ja, ich denke, dass der Staat das schon kritisch sieht, dass er sein Monopol ein bisschen untergraben sieht an der Stelle. Sehe ich schon. Ich denke aber schon, dass es noch sehr lange dauern wird, bis echte Maßnahmen ergriffen werden. Vielleicht so lange, dass es fast zu spät ist. Aber es ist natürlich auch hier der Aspekt der Spieltheorie. Ähnlich wie bei der Steuerflucht herrscht ja immer ein gewisser Wettbewerb zwischen den Nationen. Wenn Deutschland jegliche Steuerflucht

bekämpfen würde, gäbe es deutlich weniger Unternehmen in Deutschland. So ähnlich wird es auch mit Kryptowährungen sein. Es herrscht auch ein gewisser Widerspruch. Als Staat will man sein Monopol innehaben, aber auf der anderen Seite will man auch die ganze Wirtschaft, die um Kryptowährungen entsteht, nicht ausschließen. Man will seine Währung schützen, aber man will nicht unbedingt Protektionismus betreiben, der, wie wir wissen, auch nicht immer gut ist [lacht]. An der Stelle wird es immer so ein gewisses Spiel geben. Einige Staaten werden versuchen Währungen (Anmerkung des Autors: Kryptowährungen) zu verbieten und werden dadurch gewisse wirtschaftliche Nachteile haben, andere Staaten werden alles zulassen und ähnlich wie jetzt in der Schweiz, die jetzt mit dem Kryptovalley-Zug natürlich enorme Vorteile haben, wenn sie die Krypto-Gemeine sozusagen mit offenen Armen empfangen. Ich glaube, dass es unrealistisch ist, dass ein Staat oder die ganze Welt Kryptowährungen verbieten könnte. Dazu sind sie einfach großwirtschaftlich zu profitabel. #00:33:35-9#

I: Alles klar, das waren alle meine Fragen. Dann bedanke ich mich herzlich für das Interview. #00:33:44#

Eidesstattliche Erklärung

Ich, _____

geboren am _____

erkläre hiermit, die vorliegende Bachelorarbeit selbständig und ohne fremde Hilfe angefertigt zu haben. Dabei habe ich mich keiner anderen Hilfsmittel bedient als derjenigen, die im beigefügten Quellenverzeichnis genannt sind.

Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind von mir als solche kenntlich gemacht.

....., den …… .....
Studienort Unterschrift Studierende/r (= Verfasser/in)